IT biztonság közérthetően



Neumann János Számítógép-tudományi Társaság

Erdősi Péter Máté, CISA
Solymos Ákos, CISM, CRISC

IT biztonság közérthetően

verzió: 3.0
2018. augusztus

Kiadja a Neumann János Számítógép-tudományi Társaság (NJSZT)

Készítette a Neumann János Számítógép-tudományi Társaság
megbízásából az Időérték Oktatási, Kereskedelmi és Tanácsadó Kft. és az NFS Informatikai és Szolgáltató Bt.

Erdősi Péter Máté CISA és Solymos Ákos CISM, CRISC

Lektor: Zengő Andrea CISA, CISM, CISSP

Kiadó: Neumann János Számítógép-tudományi Társaság
1054 Budapest, Báthory u. 16.

Felelős kiadó: Alföldi István CGEIT, ügyvezető igazgató NJSZT

ISBN: 978-615-5036-12-5

A könyv elkészítését
a QUADRON Kibervédelmi Szolgáltató Kft.
és a BlackCell Kft. támogatta

Tartalomjegyzék

Ábrajegyzék

1 Bevezetés

A bennünket körülvevő, rohamosan változó világ kihívásaihoz nélkülözhetetlen információkkal frissített könyvet tart kezében a Kedves Olvasó.

Kitűzött és mindenki számára nyilvános célunknak megfelelően jelentősen, az élet és az információs társadalom fejlődésével összhangban aktualizáltuk **IT biztonság közérthetően** című kötetünket.

„A fejlődés ellen nincs gyógymód” – mondta **Neumann János** a múlt század ötvenes éveiben. Ma már az ezzel járó felelősségre is felhívná a figyelmet.

Az idén 50 éves Neumann János Számítógép-tudományi Társaság (NJSZT) jelmondata - „**Tudás, Elkötelezettség, Felelősség**” - kötelezi a társaságot a civil társadalom infokommunikációs világban való eligazodásának maximális támogatására. E jubileumi évben is kiemelt célunk, hogy az információs társadalom valamennyi szereplőjét megszólítsuk.
A könyvet a téma kiváló szakemberei írták – és a téma fontossága miatt a könyv elkészítésében az NJSZT együttműködött a *Nemzeti Kibervédelmi Intézet*tel, valamint a *Nemzeti Közszolgálati Egyetem*en alakult *Kiberbiztonsági Akadémiával*.

Az NJSZT a civil társadalom iránti felelősség jegyében továbbra is mindenki számára *ingyenesen hozzáférhető* könyvvel igyekszik segíteni abban, hogy minden állampolgár felelős módon használja az infokommunikációs eszközöket.

Akik már letöltötték könyvünk valamelyik előző változatát, biztosak lehetnek benne, hogy ez a változat számos olyan új információt tartalmaz, amely a kornak való megfeleléshez nélkülözhetetlen.

Kötetünk *első öt fejezete* a legfontosabb alapinformációkat és veszélytípusokat tekinti át. A *6. fejezet* foglalkozik részletesen a különböző esetekben alkalmazható/alkalmazandó védelem ismertetésével. A *7. fejezetben* található *Ajánlott irodalom* egyes elemeinek keletkezési dátuma ugyan több esetben „réginek” tűnhet, az ajánlott művek ettől függetlenül nem elévülő alapvetéseket tartalmazó, hasznos szemléletformálók. E mellett az Olvasó a kötet tanulmányozása közben számos fontos *link*kel találkozhat, melyek az IT biztonság legaktuálisabb kérdéseihez szolgáltatnak friss példákat.

Akár régi, akár új olvasót köszönthetünk Önben, őszintén javasoljuk, hogy merüljön el könyvünk világában. Ugyanis olyan világban élünk, ahol életünk valamennyi, legapróbb része is az infokommunikáció látható vagy láthatatlan együttműködését igényli. Naponta olvasunk zsarolóvírusokról, amelyek pénzt követelnek azért, hogy számítógépünket vagy okos

eszközünket tovább használhassuk. Naponta olvashatunk hackertámadásokról, amelyek jobb esetben csak egy-egy megcélzott közösségi portált törnek föl, rosszabb esetben akár kiberháborút is jelenthetnek.

Miközben ma már az életünk nagy részét a közösségi oldalakon töltjük, magunkról mindenféle információt megosztva, interneten bankolunk, webáruházakban vásárolunk – és ezek mind törekszenek is arra, hogy biztonságos környezetet teremtsenek, mégis egyre több és professzionálisabb veszélyeztetésnek is ki vagyunk téve, ha nem vagyunk elegendően körültekintőek. Könyvünk alapvetően azt a célt szolgálja, hogy mindenki, különösebb kötöttség nélkül áttekinthesse a veszélyeket és a „kockázatokról és mellékhatásokról” ne kelljen nem várt események bekövetkezése után tájékozódnia.

Megújított könyvünkben részletesebben kitérünk az e-mailen érkező kártevők, adathalászat felismerésére, a PC/laptop használatánál is gyakoribb okostelefonozás kihívásaira, a bankkártyás és internetes fizetési lehetőségek biztonsági kérdéseire, a fake news, a *kattintásvadászat* veszélyeire és e veszélyek felismerésére. Létfontosságú, hogy ne engedjük, hogy megtévesszenek, befolyásoljanak minket – vagy hogy adatainkat, akár pénzünket is ellopják.
Különösen fontosak ezek a készségek abban a világban, amely törvényt is alkotott az információs biztonságról, sőt az Európai Unió idén be is vezette a **GDPR**-t (General Data Protection Regulation), amelynek kérdését a korábbi kiadásban csak érintettük, most külön alfejezetet szentelünk (6.1) neki.

A könyvben összefoglalt ismeretek nemcsak arra alkalmasak, hogy a napi gyakorlatban segítsenek elkerülni a rendszereknek sérülést okozó hibákat, hanem arra is, hogy az ECDL informatikai biztonság moduljának tankönyvéül szolgáljanak.

Az ECDL az informatikai írástudás felhasználói szintű keretrendszere, amelyet Magyarországon eddig már több mint félmillió ember megismert, és a több mint tíz moduljából az egyik nem véletlenül az informatikai biztonság.

Kedves Olvasó! Akár digitális írástudásának átfogó fejlesztése a célja, akár az, hogy mindennapi eligazodását megkönnyítse, feltétlen tanulmányozza át alaposan kötetünket. Minden visszajelzést szívesen fogadunk – még a kedvezőeket is! – a titkarsag@njszt.hu címen.

Budapest, 2018. augusztus

Alföldi István, *CGEIT*
ügyvezető igazgató
NJSZT

2 Biztonsági alapfogalmak

2.1 Biztonság

Az élet számos területén sokszor használjuk azt a fogalmat, hogy „**biztonság**". De mit is értünk alatta? Mit jelent például a létbiztonság? Azt, hogy a mindennapi életünk alapjai a jelenben megvannak (nem éhezünk és van hol laknunk) és a jövőben sem várható ebben jelentősebb mértékű változás. Hasonló értelemben szoktuk használni a „közbiztonság" fogalmát is – ha a környezetünkben elvétve fordul elő bűncselekmény, akkor jónak érezzük a közbiztonságot, viszont ha minden nap kirabolnának valakit az utcánkban, akkor előbb-utóbb elkezdenénk félni attól, hogy ez velünk is megtörténhet, és sürgősen szeretnénk a közbiztonságot javítani. Valahol mindkét esetben arról van szó, hogy a biztonság a szubjektum számára egy kedvező állapot, amelynek megváltozását nem várja, de nem is tudja kizárni. Idealizált, édenkerti esetben ez az állapot örökkön-örökké fennmaradhat. Azonban világunk nem ideális, ezért minden időpillanatban számos **veszély** fenyegeti a biztonságot. Annyira érezzük magunkat biztonságban, amennyire a körülöttünk lévő világ képes megelőzni és felismerni a fenyegetéseket, illetve javítani a bekövetkezett események káros hatásait. Ha elfogadjuk, hogy biztonság akkor van, ha a fenyegetettség minimális, akkor a biztonság a sérülékenységek hiányát vagy a fenyegetésekkel szembeni védelmet jelenti[1].

A biztonság tehát a minőség és a megbízhatóság mellett a harmadik olyan követelmény, amelyet figyelembe kell venni a hosszútávú működés fenntartása szempontjából. Hétköznapi értelemben a biztonság veszélyektől mentes, zavartalan állapotot jelent[2]. Az informatikai rendszerek esetében a legfontosabb az adatok biztonságát megvalósítani. Három **adatbiztonsági követelmény** létezik:

- **bizalmasság:** valami, amit csak az arra jogosultak ismerhetnek meg, korlátozott a megismerésre jogosultak köre.
- **sértetlenség vagy integritás:** valami, ami az eredeti állapotának megfelel és teljes.
- **rendelkezésre állás:** a szükséges infrastruktúrák, valamint adatok ott és akkor állnak a felhasználó rendelkezésére, amikor arra szükség van.

---

[1] http://uni-nke.hu/downloads/kutatas/folyoiratok/hadtudomanyi_szemle/szamok/2013/2013_4/2013_4_alt_urmosi.pdf

[2] Magyar Értelmező Kéziszótár, Akadémiai Kiadó (1978), 139. oldal

Ha egy szemléletes példával szeretnénk illusztrálni a fenti hármas követelményt, akkor arra talán a szervezeteknél megtalálható fizetési lista lenne a legjobb. Bizalmasság: a fizetési információk jellemzően érzékeny adatok, senki sem szeretné, ha az arra feljogosítottakon túl mások is látnák azt, hogy mennyi a fizetése. Sértetlenség vagy integritás: komoly probléma lenne, ha a fizetési adatokat valaki illetéktelenül módosítaná, valakinek csökkentené, valakinek pedig emelné a fizetését. Végül a rendelkezésre állás: ha valaki letörölné vagy egyéb módon elérhetetlenné tenné a bérlistát és a dolgozók nem kapnának fizetést, az komoly problémát okozna. A fenti hármas követelmény biztosítása érdekében hozunk számos védelmi intézkedést.

A tárgyban további négy fogalmat is szoktak használni, amelyek értelmezése olykor nem egyértelmű [a]:

- **adatbiztonság:** a számítógépes rendszerekben tárolt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának megteremtése (nem foglalkozik az alkalmazások és a kisegítő berendezések – pl. szünetmentes áramforrás – biztonságával)
- **informatikai biztonság:** az információs rendszerekben tárolt adatok és a feldolgozáshoz használt hardveres és szoftveres erőforrások biztonságára vonatkozik. Ha az „adat” fogalmát kiterjesztjük az „információ”-ra, akkor ez a definíció egyenértékű az információbiztonság fogalmával, egyébként szűkebb értelmű nála.
- **információbiztonság:** tények, utasítások, elképzelések emberi vagy gépi úton formalizált, továbbítási, feldolgozási vagy tárolási célú reprezentánsai bizalmasságának, sértetlenségének és rendelkezésre állásának megteremtése. Amennyiben az „adat” fogalmába beleértjük az emberi formalizálást is (beszéd, előadás, beszélgetés), akkor egyenértékű az informatikai biztonság fogalmával, egyébként bővebb nála.
- **adatvédelem:** személyes adatok jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége[3]

[3] https://www.naih.hu/adatvedelmi-szotar.html

2.2 Kibertér

Miért jelentkezik ma már társadalmi szinten az információbiztonsági igény? Mert a mai társadalmi rendszerek – ideértve a gazdaságban, a kormányzatban, önkormányzatban és otthon működő rendszereket egyaránt – függenek az információtechnológiától, és ez a függés az egyes rendszerek összekapcsolódásával, a **kibertér** létrejöttével világméretűvé vált.

Magyarország is felismerte a kibertér fontosságát, ezért megjelent Magyarország Nemzeti Kiberbiztonsági Stratégiája is, az 1139/2013. (III. 21.) Kormányhatározat [1] formájában.

A stratégia a kibertér fogalmát így definiálja:

„A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információ rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti. Magyarország kibertere a globális kibertér elektronikus információrendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve amelyekben Magyarország érintett.”

Nem hagyható ki a kibertér fogalmából a „kutatási, felsőoktatási és közgyűjteményi hibridhálózat” és az arra épülő informatikai rendszerek, amelyek fejlesztője és üzemeltetője a NIIF (Nemzeti Információs Infrastruktúra Fejlesztési Program)

2.3 Nemzeti Kibervédelmi Intézet

A Nemzeti Kibervédelmi Intézet (NKI) látja el Magyarországon a hatósági, biztonságirányítási, sérülékenység-vizsgálati és CERT feladatokat - alapvetően az állami és önkormányzati szervek vonatkozásában. Ezen komplex feladatkörének köszönhetően az Intézet az előbb említett szervezeteknél üzemelő elektronikus információs rendszerek teljes információbiztonsági életciklusára vonatkozóan rendelkezik feladatkörrel. Ezen túlmenően nyomon tudja követni és segíteni tudja azok alakulását, beleértve a tervezési szakaszt, a szabályozást, az ellenőrzést, valamint az incidenskezelést egyaránt.

Az NKI részét képező Kormányzati Eseménykezelő Központ az országon belüli koordinációs szervezeteként végzi az internetet támadási csatornaként felhasználó incidensek kezelését, illetve elhárításuk koordinálását; továbbá közzéteszi a felismert és publikált szoftver

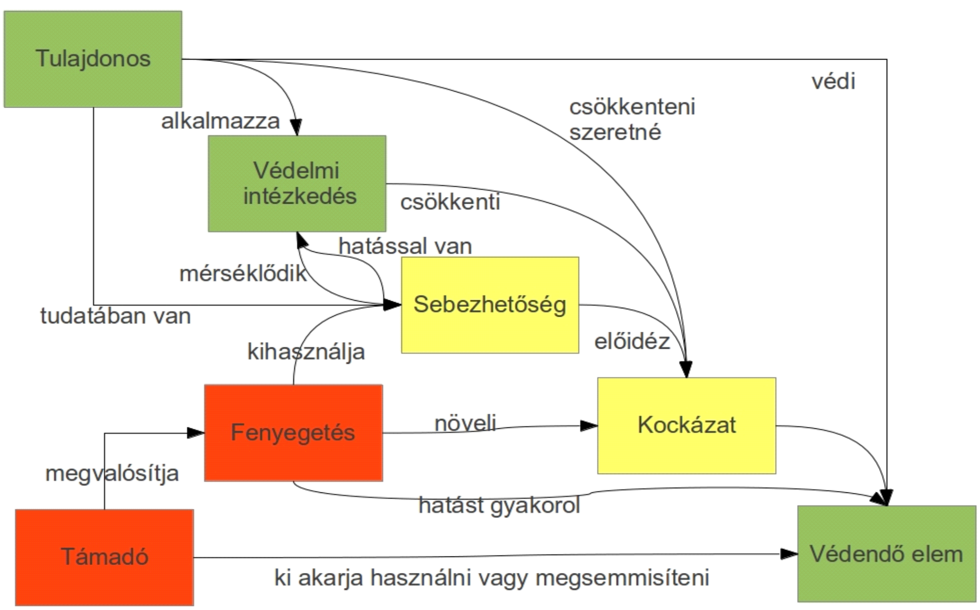
sérülékenységeket. Főbb feladatai fentieken kívül a biztonsági események kezelése, ügyeleti szolgálat, elemzés/értékelés, kibervédelmi gyakorlatok, képzések, tudatosítási programok és sérülékenység vizsgálatok végrehajtása.

A Nemzeti Kibervédelmi Intézet rendeltetése, hogy előmozdítsa a kormányzati szektor elektronikus informatikai rendszerei biztonsági szintjének emelését, valamint, hogy fejlessze a közigazgatásban dolgozó felhasználók biztonságtudatos viselkedését a kibertérben. Nemzetközi és hazai partnerkapcsolatai révén az NKI hozzájárul a teljes magyar kibertér biztonságának erősítéséhez.

További információ az Intézetről a http://www.govcert.hu/ [b] és a http://neih.gov.hu [c] oldalon olvasható.

2.4 A biztonság koncepcionális megközelítése

A Common Criteria [2], melyet szoftverrendszerek biztonsági értékelésére dolgoztak ki – és amely ISO/IEC 15408 szabványként is ismert - a biztonság teljeskörű koncepcióját a 2.3 verziójában fogalmazta meg a rendszerek tulajdonságait is figyelembe véve. A koncepció tartalmazza a támadót, a támadásokat, a védelmet megvalósító tulajdonost, a védelmi intézkedéseket és a védendő elemeket egyaránt.



1. ábra Biztonsági koncepció

Az ábrán szereplő fogalmak definícióit a következőkben adjuk meg [3] felhasználásával:

- **Védelmi intézkedés:** a fenyegetettség bekövetkezési valószínűségének csökkentésére, illetve a bekövetkezéskor jelentkező kár csökkentésére szervezési vagy technikai eszközökkel alkalmazott intézkedés. Például: tűzfalak, végpontvédelem, biztonsági szabályzatok bevezetése, felhasználók oktatása, beléptető rendszer stb.

- **Sebezhetőség:** A veszélyforrás képezte sikeres támadás bekövetkezése esetén a védendő elemek sérülésének lehetősége. Más szóval a védendő rendszer olyan tulajdonsága, amelyben rejlő hiba, hiányosság kihasználásával a támadó sikeres támadást hajthat végre az adatok, rendszerek, szolgáltatások vagy egyéb erőforrások ellen.

- **Támadás:** A támadás egy, az erőforrások bizalmassága, sértetlensége és/vagy rendelkezésre állása ellen irányuló, többnyire egy vagy több sebezhetőségből kiinduló, valamilyen fenyegetést megvalósító folyamat.

- **Fenyegetés:** A fenyegetés a támadás lehetősége, vagy a biztonság megsértésének lehetősége; amely a támadás tárgyát képező erőforrásra irányul.

- **Kockázat:** A kockázat annak a lehetőségnek a valószínűsége, hogy egy fenyegetés támadás útján kárkövetkezményeket okoz. Kárkövetkezmény lehet anyagi, jogi, reputációs, humán erőforrást stb, érintő. A kockázati érték meghatározásánál adott fenyegetettség bekövetkezési valószínűségét és az általa okozott kárkövetkezmény nagyságát szokták alapvetően figyelembe venni. Különböző módszertanok ettől eltérő számítási metódusokat is használnak.

- **Védendő elemek:** a szervezet vezetősége (menedzserei) által meghatározott küldetést/üzleti célt vagy társadalmi célt megvalósító erőforrások összessége, ideértve az informatikai feladatok végrehajtásához rendelt embereket, eszközöket (informatikai és egyéb), dokumentumokat, fizikai telephelyeket, folyamatokat és nem utolsó sorban az adatokat.

Az ábrából a fenti definíciókra támaszkodva a következő koncepcionális állítások olvashatók ki:

- A támadó rosszindulatú tevékenységeket akar végezni a védendő elemeken.
- A tulajdonos meg akarja védeni a védendő elemeit.

- A tulajdonos tisztában van a sebezhetőségekkel, ezért védelmi intézkedéseket alkalmaz.
- A védelmi intézkedések csökkentik a kockázatokat.
- A sebezhetőségek idézik elő a kockázatokat.
- A védelmi intézkedések hatnak a sebezhetőségekre, mérséklik azok hatását a védendő elemekre nézve, úgy, hogy vagy mérséklik a támadások kárkövetkezményeit, vagy csökkentik azok bekövetkezési valószínűségét.
- A támadó igyekszik megvalósítani a fenyegetés bekövetkezését, ami növeli a kockázatot.
- A fenyegetések a sebezhetőségeket használják ki.

A támadások működési mechanizmusa tehát az, hogy a támadó megkeresi a védeni kívánt informatikai rendszer sebezhetőségeit, amelyeken keresztül támadásokat próbál meg realizálni. A tulajdonos a kockázatokat védelmi intézkedésekkel csökkenti, melyek lefedik a sebezhetőségek által jelentett gyengeségeket. A biztonság innentől kezdve mérhető, mégpedig a sikeres támadások számával, valamint a kárkövetkezmények és a védelemre fordított erőforrások számszerűsítésével. Ugyanakkor fontos kijelenteni, hogy 100%-os biztonság nem létezik. Amennyiben egy kockázatot teljesen meg szeretnénk szüntetni, akkor azt jellemzően a védendő erőforrás, rendszer vagy szolgáltatás megszüntetésével lehet elérni.

Maga a folyamat, amely a fent megismert koncepciót valósítja meg, az a kockázatkezelés. A kockázatkezelés során a szervezet felméri, milyen fenyegeték irányulnak a szervezet eszközei ellen, amelyek lehetnek rendszerek, adatok, telephelyek és maga a felhasználó is. Azt is megbecsülik, hogy ezek a fenyegetések mennyire valószínű, hogy bekövetkeznek, és ha bekövetkeznek, akkor milyen hatással járnak. Több hatás mentén is lehet mérni a kárkövetkezményeket, hogy minél pontosabb képet kapjon az értékelő, hogy milyen hatással lehet az adott fenyegetés a szervezetre. Az így kapott információ mutatja a kockázatokat, amelyek kapcsán négyféle koncepció mentén dönthet a szervezet azoknak a mérsékéséről:

- Kockázatcsökkentő intézkedések foganatosítása, azaz olyan kontrollokat alkalmaz, amelyek csökkentik a bekövetkezés valószínűségét, esetleg a hatásait.
- Kockázat elkerülését is választhatja, ha például egy kockázatosnak ítélt tevékenységet nem követ, így a kockázat is megszűnik.

- Kockázat kapcsán áthárítást is választhat, azonban ebben az esetben nem a kockázatot, hanem annak hatását hárítja át. Tipikusan ide tartoznak a biztosítások.
- Kockázatot el is lehet fogadni, amennyiben a szervezet úgy dönt, hogy a kockázat hatása számára elfogadható szinten van, nincs szükség további intézkedésekre.

Nézzük ezt egy gyakorlati példán keresztül. Az a tervünk támad, hogy a családdal síelni megyünk. Autóval szándékozunk menni, és azt is tudjuk, hogy síelni nem igazán tudunk. A kockázat, amit értékelünk, egy esetleges lábtörés. Mit tehetünk, hogy a felmerülő kockázatokat csökkentsük? Van néhány lehetőség előttünk:

- Elmegyünk oktatásra és felkészülünk a kihívásra. Ez egy kockázatcsökkentő intézkedés.
- Biztosítást kötünk. Amennyiben az oktatás ellenére is közelebbről megismerkedünk a hóval, a mentés költségeit a biztosítóra hárítjuk. (A kárt nem, mert mi leszünk a sérültek.)
- Elfogadjuk a kockázatot, és bízunk a szerencsénkben.
- Elkerüljük a kockázatot, inkább nyáron megyünk a tengerpartra.

2.5 Információkritériumok

Az informatikai rendszerek használatának minden esetben valamely konkrét célja van, nem öncélú. A folyamatok bemeneteik és kimeneteik előállításához információs rendszereket használnak, amelyek működése információtechnológiai, vagyis informatikai hardver- és szoftver-alapú megoldásokat igényelnek. Ennek következtében a folyamatok informatikai függése – és ebből adódóan az energiafüggése is – kialakul. Ezek nélkül a gyakorlatban már nem tudják az információfeldolgozásra épülő feladataikat ellátni.

Az információs rendszerek **információkat** dolgoznak fel. Az információ fogalmának meghatározása az adatfeldolgozás fejlődésével együtt változott. Amíg azt gondolták, hogy értelmező tevékenységet csak az ember képes végrehajtani, addig az információt csak az emberi agyban létezőnek ismerték el. Miután felismerték az egyes biológiai rendszerek információ-feldolgozási képességét (pl. DNS, dezoxiribonukleinsav), illetve megjelentek a számítógépek és elkezdtek gyorsan, nagy tömegű adatot feldolgozni; ez megváltozott és új tudományterületek kialakulásához vezetett (pl. információtörténet, kommunikáció-elmélet, információ-fizika, adatbázis-kezelés, adatbányászat). Az információ szó hallatán rendezett adatokra vagy összefüggő minta szerint rendezett tényekre utalunk, amelyek között általában nincs éles határvonal. A rendezettség más szóval azt jelenti, hogy az információ

minden esetben valamely adatfeldolgozási művelet eredményeként áll elő, hiszen a rendezettséget valahogyan el kell érni.

Az információs rendszerek használatának a célja valamely társadalmi, gazdasági vagy magánszféra folyamat támogatása bemeneti-kimeneti információkkal; illetve azokelőállítási képességével. Az információk minősége között azonban lehetnek különbségek, melyek erőteljesen befolyásolják a cél mennyiségi és minőségi elérhetőségét. Ezeket a különbségeket az **információ-kritériumok** alapján lehet megérteni.

A célkitűzések elérése érdekében az információknak ki kell elégíteniük bizonyos kontrollkritériumokat. A szélesebb körű minőségi, pénzügyi, megbízhatósági, és biztonsági követelmények alapján az alábbi hét megkülönböztethető, egymást néhol minden bizonnyal átfedő információ-kritérium került meghatározásra a szakirodalomban (COBIT 4.1 [4]):

- **hatékonyság:** arra vonatkozik, hogy az információkat az erőforrások optimális (legtermékenyebb és leggazdaságosabb) kihasználásával biztosítsák
- **hatásosság/eredményesség:** azzal foglalkozik, hogy az információk a folyamat szempontjából jelentőséggel bírnak, és hogy az információkat időben, helyes, ellentmondásmentes és használható módon biztosítsák
- **megfelelőség:** a folyamatokat érintő törvények, jogszabályok, szabályozások és szerződéses megállapodások – azaz kívülről előírt jogi és önként vállalt követelmények és belső irányelvek – betartását jelenti, amelyeknek a folyamat a tárgyát képezi
- **megbízhatóság:** a vezetés számára olyan időszerű és pontos információk biztosítása, amelyek az adott szervezet működtetéséhez, pénzügyi megbízhatóságához és irányításához szükségesek
- **bizalmasság:** arra vonatkozik, hogy megakadályozza, a bizalmas információk engedély nélküli megismerését, vagyis fontos információkhoz illetéktelenek ne férjenek hozzá
- **sértetlenség:** az információknak a szervezeti értékek és elvárások szerinti pontosságára, változatlanságára és teljességére, valamint az információk érvényességére vonatkozik

- **rendelkezésre állás:** azzal foglalkozik, hogy az információk akkor álljanak rendelkezésre, amikor azokra a folyamatnak szüksége van most, és a jövőben; a szükséges erőforrások, és az erőforrások szolgáltatási képességeinek védelmére is vonatkozik

Az információ felhasználhatóságára vonatkozik az első négy kritérium, a biztonságra pedig az utolsó három. Minden **információbiztonság**i törekvés arra irányul, hogy a három biztonsági követelménynek való megfelelőséget minden időpillanatban biztosítsa az összes védendő információra és környezetükre egyaránt. Egy szervezet akkor mondhatja el magáról, hogy biztonságtudatosan működik, ha a felhasználók és az egyéb szerepkörökben dolgozók tudatában vannak az alapvető és esetleg szervezetspecifikus fenyegetettségeknek, képesek ezeket felismerni és tudják, hogy mi a teendő egy felismert vagy gyanított incidens esetén, milyen csatornán tudják bejelenteni és felhasználóként mi a követendő magatartás az egyes események kapcsán. Ehhez az állapothoz hosszú út vezet, a szervezet biztonsági kultúráját meg kell teremteni. Felhasználóként tudatában kell lennünk, hogy mi vagyunk az első és legintelligensebb védelmi vonala a szervezetnek, és hogy a biztonság mindenki érdeke, a cég jövője és a munkahely biztonsága múlhat rajtunk.

3 Információrendszerek

Az információnak **életciklusa** van, ahogyan azt a COBIT 5 megfogalmazta [5]. Az életciklus arra fókuszál, hogy a működtetett folyamatok hogyan képesek azt az értéket előállítani, aminek az érdekében ezeket a folyamatokat létrehozták. Nagyon fontos megállapítás az, hogy a létrehozni kívánt értékek előállításhoz tudás szükséges, amihez a megfelelő információk nélkülözhetetlenek. Az információkat adatok feldolgozásával állítjuk elő, az **adat**ok pedig információs rendszerekben jönnek létre, tárolódnak és itt dolgozzák fel őket.

Az információs rendszerek **számítógépes architektúrákon** [d] működnek, ideértve mind a hardveres, mind a szoftveres környezetet. A szoftveres környezet a virtualizáció fejlődésével jelentős átalakuláson ment keresztül. Korábban a hardver és az alkalmazás nem volt nagyon távol egymástól, ma már több virtuális szint is létezhet az egyes számítógépes architektúrákban, anélkül, hogy ebből a felhasználó bármit is észrevenne.

Az egyes számítógépek összekapcsolási módja is megváltozott, a vezeték nélküli technológiák jelentős teret nyertek minden szektorban a hálózatok kialakítása terén a

vezetékes átviteli technológiák mellett – ez a trend új fenyegetéseket is hozott be a mindennapjainkba.

3.1 Hardveres infrastruktúra

A számítógépes architektúrákat két alapvető részre szokás felbontani: hardverre és szoftverre. A **hardverek** adják a számítási műveletek fizikai hátterét a szükséges adat-beviteli és kimeneti egységekkel együtt. Ezeken a hardvereken pedig különböző szintű programokra lesz szükség a **szoftveres** adatfeldolgozási feladatok ellátására.

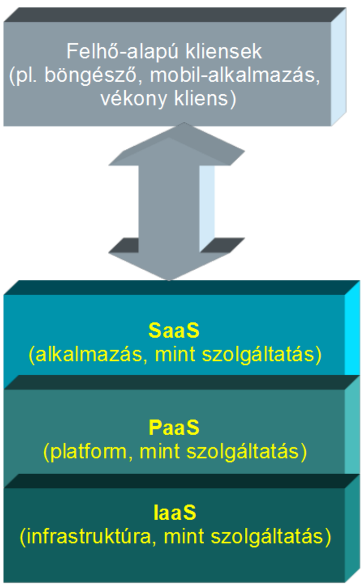
Felépítésükben nem különböznek, de feladatuk különböző, ezért meg lehet különböztetni az adatok feldolgozására szolgáló **számítógép**eket, adatbázis-szervereket, adattárházakat a kommunikációra szolgáló hardverektől (jelismétlő, híd, útválasztó). Kliens-szerver architektúrában két oldal jelenik meg: a kiszolgáló architektúra és a kliens-oldal, ezeket a speciális körülményeket figyelembe vevő programok működtethetők rajtuk.

3.2 Alkalmazások, szolgáltatások

A hardveres egységek összeszerelésüket követően még nem képesek szofisztikált felhasználói utasításokat végrehajtani, ezeket teszik majd lehetővé a különböző programok, szoftverek, alkalmazások. Anélkül, hogy mély technikai részletekbe mennénk, megemlítjük, hogy a hardverek működtetéséhez az úgynevezett meghajtók, vezérlőprogramok – driverek – szolgálnak. A számítógép-architektúra teljes funkcionalitásának kihasználását az operációs rendszer teszi lehetővé, míg a felhasználók által igényelt egyes funkciókat megvalósító alkalmazásokat valamely magas szintű programozási nyelven írják és erről fordítják le a számítógép központi feldolgozó egysége által érthető futtatható kódú programmá. Ilyen program például egy szövegszerkesztő, amely a billentyűzet segítségével bevitt karaktersorozatot összefüggő és formázott szövegként képes tárolni, illetve elvégzi a mások által rögzített szövegek megjelenítését is.

Fejlesztések esetén elengedhetetlen, hogy a funkcionális követelmények mellett a biztonsági (ún. nem funkcionális) követelmények is meg legyenek határozva a fejlesztés legkorábbi szakaszától. Ennek elmaradása és/vagy nem megfelelő teszteltsége okozza azokat a szoftveres sérülékenységeket, amelyek révén a támadók megpróbálják a különböző informatikai rendszereket megtámadni, feltörni, divatos kifejezéssel élve „meghekkelni”. De ezeket a sérülékenységeket használják ki az automatizált robotok, amelyek sérülékeny weboldalak kezdőoldalait cserélik le (deface), illetve azon kártevők (vírusok, trójai programok), amelyek a felhasználókat is veszélyeztetik.

A kibertér és a virtualizáció fejlődésével megszületett az igény, hogy a felhasználók ne csak a saját gépeiken legyenek képesek szoftvereket futtatni, hanem legyen lehetőségük a különböző alkalmazásokat távolban, a **felhőben** futtatni és csak az adatokat mozgatni a helyi és a távoli számítógépek között. Ez a technika odáig fejlődött, hogy lehetőségünk van a böngészőnkön keresztül igénybe venni egy teljes virtualizált számítógépes felületet (Platform as a Service, PaaS) vagy egy szoftvert (Software as a Service, SaaS) illetve egy infrastruktúrát is (Infrastructure as a Service, IaaS) [e]. És sajnos kialakult az a szolgáltatási infrastruktúra, ahol a korábban komoly informatikai ismereteket igénylő számítógépes bűnözéshez kapcsolódó szolgáltatásokat (vírusterjesztés, szolgáltatás-megtagadásos támadások, spamküldés, informatikai rendszerek feltörése stb.) lehet elérni, gyakorlatilag bárki számára. Ez a Fraud as a Service, Faas. Ezt a témát azonban jelen tankönyv nem tárgyalja részletesen, de jó, ha a felhasználó is tisztában van vele, hogy létezik.



2. ábra Felhő alapú szolgáltatások

Néhány példa az egyes szolgáltatási típusokra:

- **SaaS:** e-mail felület, virtuális desktop, játékok, kommunikáció
- **PaaS:** adatbázisok, fejlesztési környezetek, webszerverek
- **IaaS:** virtuális gépek, szerverek, tárolók, terhelés-elosztók, hálózat

A felhasználók számára mindez azt jelenti, hogy képesek többnyire telepítés nélkül, böngészőn keresztül akár egy irodai szoftvercsomag funkcionalitását kihasználni (pl. GoogleDocs), komplex kommunikációs (telefonálás, levelezés, azonnali üzenetküldés) szolgáltatásokat felhasználni (pl. Skype, Viber, Whatsapp, Gmail) vagy közösségi oldalakon információkat, fájlokat megosztani és megkapni (pl. Facebook, Twitter, Instagram stb.). A **fájl-megosztás** saját gépről is történhet és lehetőség van már nagyméretű fájlok megosztására is (Pl. Mammutmail, Toldacuccot) valamint a fájljaink felhőben való tárolására is, (Pl. GoogleDrive, Dropbox, OneDrive). Ezen szolgáltatások használata előtt érdemes elolvasni az Általános Szerződési Feltételeket. Ebben van leírva, hogy a szolgáltató mit szolgáltat, miért vállal és miért nem vállal felelősséget, ki férhet hozzá adatainkhoz és így tovább. Fontos tudni továbbá, hogy az egyes szolgáltatók ingyenes és fizetős, illetve akár vállalati felhasználásra szánt szolgáltatásai között jelentős különbségek lehetnek, biztonsági szempontból is.

Érdemes megismerkedni a CaaS – City as a Service fogalmával, hiszen pár éven belül tapasztalni fogjuk, hogy a mindennapi életünkben is meg fognak jelenni az okosvárosok szolgáltatásai. És rajtunk felhasználókon is múlni fog a biztonságuk. A CaaS számos innovatív információtechnológiai fejlesztést integrál, hogy a városaink élhetőbbek, gazdaságosabbak legyenek. Ilyen szolgáltatások a teljesség igénye nélkül: a közösségi közlekedés optimalizálása, megosztott autó használat, közösségi terek menedzsmentje, kulturális értékek szélesebb körű elérése, köztéri információs rendszerek és nyilvános szolgáltatások adatgyűjtései és értékelése, várostervezési megfontolások és még sorolhatnánk. Ahhoz azonban, hogy ezen szolgáltatások valóban az emberek érdekeit szolgálják, a biztonsággal is kiemelt szinten kell foglalkozni.

3.2.1 Elektronikus ügyintézés

Magyarországon az egykapus ügyintézési felületet a https://magyarorszag.hu [g] portál biztosítja, ahol egy hiteles regisztrációt követően (bármelyik okmányirodában, kormányhivatali ügyfélszolgálati irodában, adóhatóság ügyfélszolgálatán, külképviseleten vagy elektronikusan indíthatja el 2016. január 1-jét követően kiállított érvényes e-személyazonosító igazolvány birtokában) számos ügy kezdeményezésére van már lehetőségünk teljesen elektronikus formában és több államigazgatási rendszerből tölthetünk le magunkkal kapcsolatosan adatokat is (pl. NAV, OEP). 2017 óta az

egészségügyi adataink, és ezen adatok kezelése kapcsán is tájékozódhatunk az Egységes Egészségügyi Szolgáltatási Térben is (EESZT).[4]

3.3 Számítógép-hálózatok

A számítógép-hálózat egy olyan speciális rendszer, amely különböző informatikai, többnyire valamilyen telekommunikációs eszközök segítségével a számítógépek egymás közötti kommunikációját biztosítja. Manapság már ideértünk minden olyan eszközt, ami a hétköznapi értelemben vett számítógépeken túl valamilyen számítógép alapú működést biztosít. Gondolva itt az okoseszközökre (okostelefon, IP kamera, autó fedélzeti számítógép, okoshűtő, okoscipő, otthon-automatizálás vezérlők stb.), valamint M2M technológiákra. A Machine to Machine (M2M) technológia olyan adatáramlást jelent, amely emberi közreműködés nélkül, gépek között zajlik.

A hálózatokat fel lehet osztani kiterjedésüket alapul véve a következő három típusra [6]:

lokális hálózatok, LAN (local area network): viszonylag kis távolságon intelligens eszközök közötti kommunikációt biztosít, erre a célra telepített fizikai kommunikációs csatornán; hatótávolsága 10 m – 5 km közötti. Ilyenek jellemzően a különböző egy telephelyes szervezeteknél, vállalatoknál és az otthon kialakított hálózatok.

nagyvárosi hálózatok, MAN (metropolitan area network): megteremti egy intézmény (gazdasági szervezet, üzem, hivatal) épületei közötti összeköttetést egy városban, vagy kb. 50 km-es körzeten belül. Hatótávolsága 1 km – 50 km közötti

távolsági hálózatok, WAN (wide area network): földrajzilag távol eső felhasználók közötti összeköttetést - jellemzően nyilvános távközléstechnikai berendezéseken keresztül - biztosító hálózat.

Nem fizikai távolság alapján különböztethető meg a többi hálózat típustól az egyre több szervezetnél használt virtuális magánhálózat (VPN – Virtual Private Network). A virtuális magánhálózat egy számítógép-hálózat fölött virtuálisan kiépített másik hálózat. „Magán” jellegét az adja, hogy a VPN-en keresztülmenő adatok nem láthatók az eredeti hálózaton, mivel titkosított adatcsomagokba vannak becsomagolva. Ez biztosítja, hogy akár a világ másik feléről is biztonságos titkosított csatornán be lehessen jelentkezni egy vállalati hálózatba és ott használni lehessen a vállalat erőforrásait (fájlszerver, üzleti alkalmazások, levelezés stb.), miközben a felhasználó fizikailag távol van.

[4] https://www.eeszt.gov.hu/

4 Fenyegetések, támadások

Az információ olyan érték, amelyek megléte vagy hiánya alapvetően befolyásolja minden folyamatunk elvégezhetőségét és eredményességét. Növelheti a hatékonyságot ha jó, és teljes használhatatlanságot vagy kiesést okoz, ha rossz. Az informatikafüggés során vált világossá, hogy a minőségi információk megléte nélkülözhetetlen a mindennapi élethez. Világos, hogy relevánsabb információval több eredmény elérésére lehetünk képesek, míg helytelen információval egyetlen folyamat sem adhat helyes és maximálisan felhasználható végeredményt. Az információt informatikai biztonsági szempontból általában az adatfeldolgozás kimenetének tekintjük, és mint ilyen, valamely számítógépes adathordozón reprezentált. De nemcsak így fordulhat elő az információ, gondoljunk csak a beszédre, a telefonos közlésekre, valamint a papír alapon tárolt információkra is, amelyeket adott esetben szintén védeni szükséges. Az információ olyan fontos és értékes elemmé vált, hogy be is épült az információtechnológiai **erőforrás**ok közé a hardver és a szoftver mellé minden keretrendszerben, szabványban. Védeni kell tehát a hardver és a szoftver mellett a fontosnak ítélt információkat is. Egyre inkább elterjedt nézet, hogy a legfontosabb erőforrás az adat. Hiszen sokszor nem megismételhető, vagy nagyon nehezen reprodukálható folyamatok, számítások alapján áll elő. Gondoljunk itt egyszerű példaként a saját családi fotóalbumunkra. Vagy arra, hogy a gyermekünk első feltápászkodásáról és első lépteiről szóló videófájl, ha nincs meg több példányban és megsérül, véletlenül letöröljük, vagy egy zsarolóvírus letitkosítja, akkor jó eséllyel soha többet nem láthatjuk viszont, mert nem megismételhető a forrásesemény. Ezzel szemben a hardver vagy a szoftver, bár pénzben kifejezve komoly értéket képviselnek, reprodukálhatók. Tudok venni egy új laptopot, újra meg tudom venni a programot rá. Az egyedi adatokról, legyenek azok dokumentumok, fotók, fájlok, hangfelvételek, már ez nem mondható el.

Ezeket az értékeket a támadók is felismerték, és támadásaikat két tényező köré csoportosították:

- **rombolás:** károkozás a megtámadottnak, a működési folyamataihoz szükséges erőforrások sérülésének előidézésével (beleértve az információt is)
- **haszonszerzés:** az erőforrások eltulajdonításával saját szakállukra megszerezni azt a hasznot, ami a más erőforrásai illegális felhasználásával elérhető (információ-lopás, zombi hálózat, stb.). Ennek minősített esete a **személyazonosság-lopás**,

amikor a haszon a támadóé, a büntetés a megtámadotté – hacsak nem tudja ártatlanságát bizonyítani. Az utóbbi években pedig első helyre lépett elő a zsarolás, amelyet a támadók zsarolóvírusok terítésével hajtanak végre. Az anyag részletesen tárgyalja majd ezt a témát.

Fenti két célt jellemzően rosszindulatú szoftverekkel és egyéb változatos támadási formákkal valósítják meg a támadók.

4.1 Rosszindulató szoftverek

Rosszindulatú szoftvereknek nevezünk minden olyan programot, amelyik a tulajdonos előzetes engedélye nélkül bármilyen tevékenységet akar végezni a számítógépeinken vagy a hálózatra feltöltött adatainkkal. A kifejezés angol változata (**malware**) a „malicious software” kifejezés rövidüléséből eredt. A rosszindulatú programkód tehát számítógépes rendszerekbe engedély nélküli beszivárgást, vagy a felhasználóknak kárt okozó nem engedélyezett tevékenységet lehetővé tévő vagy megvalósító szoftver. Ezeket károkozási célból készítik és küldik. A rosszindulatú programok elrejtésére a rendszerszinten tevékenykedő kártékony kódokat (**rootkit**) használják általában.

Az egyes rosszindulatú programokat az alábbiak szerint osztályozhatjuk:

- vírusok: olyan programok, amelyek más fájlokhoz kapcsolódva önmaguktól terjednek, vagy e-maileken keresztül küldik őket, és károkat okozhatnak a számítógépeken. Kiemelt alfajuk a zsarolóvírusok, amelyek letitkosítják a megfertőzött eszköz (munkaállomás, szerver, okostelefon stb.) fájljait és váltságdíj ellenében adják meg a titkosítás feloldásához szükséges kulcsot. Bővebben lásd: zsaroló programok.
- férgek: a vírushoz hasonló önsokszorosító számítógépes program. Míg azonban a vírusok más végrehajtható programokhoz vagy dokumentumokhoz kapcsolódnak hozzá illetve válnak részeivé, addig a férgek önállóan fejtik ki működésüket.
- trójai programok: nevüket az ókori Trója ostrománál alkalmazott hadicsel eszközéről kapták, amely révén egy legálisnak látszó letöltésben egy olyan program bújik meg, ami előbb-utóbb aktivizálódik incidenseket okozva (például hátsó kapukat tölt le vagy rosszindulatú programokat indít el).
- hátsó kapuk: szoftverekbe épített olyan kiegészítések, amelyek bizonyos kiválasztott személyek részére hozzáférést engednek az egyes programokhoz, a számítógéphez, vagy az azokon kezelt adatokhoz. A hátsó kapuk egy részét a

szoftverek fejlesztői tudatosan, szervizcélokkal építik be, míg kisebb részük programozási hiba következtében teszi lehetővé a hozzáférési szabályok kikerülését a jogosulatlan hozzáférést így megszerző támadóknak. Ezen kívül léteznek kifejezetten hátsó kapuk nyitásának céljával létrehozott támadóprogramok is, amelyeket általában vírusok, illetve kémszoftverek részeként terjesztenek a felhasználó tudta nélkül. Ezek támadási célú használata azért veszélyes, mert minden egyes esetben rosszindulatú programkódok telepítéséhez vezethet. A hátsó kapu a rendszerbiztonság megkerülésével működik, így az egyébként kialakított védelem itt nem fog érvényesülni.

- rendszerszinten rejtőző programok: olyan kártékony szoftverek, amelynek célja korlátlan, illetéktelen és rejtett hozzáférés megszerzése a számítógép erőforrásaihoz. Fontos tudni, hogy ezek a programok megkerülik a kialakított hozzáférés-védelmi rendszert, így az itt megszerzett hozzáférés a rendszer szintjén nem kontrollálható.
- szolgáltatás-megtagadási (Denial of Service, DOS vagy Distributed Denial of Services - dDOS) támadást indító programok: egy vagy több számítógépen futó program másodpercenként kérések sokaságát indítja a megadott cím felé úgy, hogy a küldött válaszokra nem kíváncsi, azt nem dolgozza fel. Így éri el azt, hogy a rendszert használó többi felhasználó a valódi kéréseire nem kap választ, a megtámadott számítógép túlterheltsége miatt. Ily módon, ha egy internetes áruházat ér például ilyen támadás, akkor ott nem lehet vásárolni, ergo tényleges bevételkiesés valósul meg.
- kémszoftver: a felhasználó tudta és engedélye nélkül valamely adatot a támadónak továbbító rejtett programok. Elrejtőzhetnek bármilyen alkalmazás-csomag részeként, ahol futtatható programok vannak. A számítógépes programok mellett megjelentek az okostelefonokra írt adatlopó programok is. A kémszoftverek akár a billentyűzet leütéseinket is naplózhatják például jelszavaink ellopása céljából, vagy a kamerán, vagy mikrofonon keresztül egyéb információkat lophatnak tőlünk – rólunk.
- zsaroló programok: a támadó olyan programot juttat be a felhasználó gépére vagy telefonjára vagy bármilyen számítógép alapú rendszerére, melyek a fertőzött eszközöket zárolják, vagy értékes állományokat titkosítanak, és ezáltal teszik azokat használhatatlanná. A program azt is állíthatja, hogy csak ellenszolgáltatás fejében

oldja fel a zárolást. Nincs garancia arra, hogy fizetés után az áldozat visszakapja az adatait.

- kriptovaluta bányász programok: a támadó olyan programot telepít a felhasználó számítógépére, telefonjára vagy egyéb eszközére – egyre gyakoribb, hogy céges hálózatok nagy teljesítményű szervereire – amely a felhasználó tudta nélkül kriptovalutát bányászik gazdájának (aki nem a felhasználó). A kriptovaluta bányászat önmagában egy legális tevékenység, ha a „bányász” a saját tulajdonában lévő infrastruktúrán teszi ezt. Felhasználói szempontból a kriptovalutabányászat közvetlen kárt nem, de közvetettet okozhat, mivel jelentősen lelassítja a programot futtató eszközt, ezáltal a felhasználói élmény sérülhet és az eszköz jelentősen több energiát fogyaszt, mint normál működés közben. Céges környezetben már komolyabb problémát is okozhat a bányászat, mivel ilyen esetekben a szervereken futó üzleti folyamatokat támogató alkalmazások belassulhatnak, esetleg le is állhatnak, ami viszont már pénzben is kifejezhető kárt jelent.
- kéretlen levelek: A „spam” elnevezést egy amerikai cég (Hormel Foods) konzervhús-készítményének nevéből kölcsönözték (Spiced Pork and Ham), amely 1937 óta létezik. Az internet világában ez lett a szokásos kifejezés a tömeges e-mailek jelölésére, egy Monthy Pyton darab nyomán. A kéretlen levelek közös jellemzője, hogy valamely terméket vagy szolgáltatást reklámoz mások informatikai erőforrásait jogosulatlanul – és többek között Magyarországon is – törvénytelenül felhasználva.
- kéretlen reklámszoftverek (adware): olyan ingyenesen letölthető és használható programok, melyek reklámokat jelenítenek meg a felhasználó gépén. Szokás őket PUP-nak is (Potential Unwanted Programs) hívni, mivel gyakran előfordul, hogy ezen programokon keresztül juttatnak el kártékony programokat a felhasználó gépére.
- zombi hálózati szoftverek: az angol kifejezés (botnet) a „ro**bot**” szóból és „**net**work” szavak összevonásából származik. Az informatikai szakzsargonban ezzel egy olyan programot jelölnek, amely távirányítással vagy automatikusan dolgozik a megfertőzött gépen. Előfordulhat, hogy a felhasználó számítógépe része egy botnet-hálózatnak és távirányítással dolgozik (dolgoztatják), anélkül, hogy a felhasználó tudna róla. Ehhez általában szükséges az online jelenlét. A zombi-hálózat szoftvere képes megfertőzni és irányítani egy számítógépet a tulajdonos engedélye nélkül. A zombi-hálózat szoftverét lehet adatlopásra, spamküldésre, vagy

más számítógépek megtámadására is használni, hiszen a felhasználó gépére észrevétlenül feltelepül és ott bármilyen tevékenységet folytathat.

A rosszindulatú programok leggyakrabban az interneten keresztül kerülnek fel a megtámadott gépre, amihez csak annyi szükséges, hogy a gép az internetre legyen kötve. Ennél sokkal ritkábban szoktak **fizikai támadó eszközöket** alkalmazni a támadók, mivel ehhez valamilyen személyes jelenlét szükséges, ami a lebukás kockázatát jelentősen megemeli. Azonban sikeresen lehet használni az alábbi eszközöket egy támadáshoz:

- **billentyűzet-leütéseket naplózó eszközök**: olyan kisméretű hardveres eszközök, melyeket a támadó a billentyűzet és a számítógép közé csatlakoztat be, és amely rendelkezik tárolókapacitással, amibe az eszköz az összes billentyűzet-leütést rögzíti. A támadó az eszköz tartalmának kiértékelésével juthat hozzá érzékeny információkhoz – tipikusan rendszeradminisztrátori jelszavakhoz vagy egyéb bejelentkezési adatokhoz.
- **rejtett kamerák**: olyan kisméretű adatrögzítő eszközök, melyek alkalmasak jó minőségű kép és hang rögzítésére. A kamerák működésüket tekintve lehetnek folyamatos vagy mozgásra/hangra aktivizálódók, vezetékes vagy rádiós jeleket továbbítók, illetve saját belső tápról vagy elektromos hálózatról működtethetők is. A támadó alkalmazhatja ezt a jelszavak vagy érzékeny információk eltulajdonítására, kifigyelés közben. Hátránya a személyes jelenlét, illetve a fizikai elhelyezés szükségessége. Egyes esetekben a támadók a számítógépek beépített vagy hozzákapcsolódó webkameráit képesek a felhasználó tudta nélkül bekapcsolni, rejtett kameraként használni és azokon keresztül adatokat ellopni a felhasználó környezetéből.

A modern kártevők már összetett funkcionalitást tartalmaznak, fenti listából akár többet is képesek szimultán végrehajtani.

4.2 Jellemző támadási formák és módszerek

A támadó szoftverek és fizikai eszközök áttekintése után felsoroljuk azokat a támadási formákat, melyek a felhasználó aktív vagy passzív közreműködésével jöhetnek létre – a teljesség igénye nélkül:

- eltérítéses adathalászat (pharming): a támadó a felhasználó egy adott weboldal felé irányuló forgalmát átirányítja a saját weboldalára (vagy az általa birtokolt, feltört

weboldalra) a felhasználó gépén egyes adatok módosításával, így a felhasználó gyanútlanul megadhatja a személyes adatait – például bejelentkezési adatok – azt gondolván, hogy a valódi oldalon van. A hamis weboldalak (ál weboldalak) egy az egyben lemásolják az igaziakat, a felhasználókat gyakran a sikertelennek jelzett bejelentkezési kísérletük után vissza is irányítják a támadók az eredeti weboldalra, hogy a gyanút még jobban eltereljék a csalási kísérletről. Az különbözteti meg az adathalászattól, hogy itt a támadó az áldozata gépére betörve módosítja annak beállításait.

- egyklikkes támadások: a támadók azt a bizalmi kapcsolatot használják ki, ami a felhasználó böngészője és a felhasználó által meglátogatott weboldal között fennáll. A támadónak a felhasználó környezetébe kell bejuttatnia a támadó kódot, amit a weboldal a felhasználó hiteles kérésének értelmez és megpróbál általában automatikusan végrehajtani. A támadás akkor sikeres, ha a támadó pontos üzenetet tud küldeni a weboldalnak és nincs olyan biztonsági szűrés bekapcsolva, mely a támadó által – ebben az esetben vakon – elküldött üzenetek hitelességét ellenőrizné.
- csatolmányokba rejtett rosszindulatú programok letöltetése: nagyon gyakori támadási forma, hogy a támadó ráveszi a felhasználót egy érdekesnek látszó csatolmány letöltésére és megnyitására, amikor a csatolmányba rejtett rosszindulatú program aktivizálódik – esetleg a látszattevékenység fennmaradása mellett (pl. dokumentum/kép megjelenítés, program futása stb.). A legtöbb zsarolóvírus és kriptovaluta bányász program így jut az áldozatok gépére.
- adathalászat (phishing): egy valódi weboldal támadók által lemásolt képének felhasználása (ál weboldal), amely kinézetében nem különbözik az eredetitől. A támadók arra használják, hogy bejelentkezési vagy személyes adatokat csaljanak ki a gyanútlan felhasználókból, miközben azt hiszik, hogy az eredeti weboldalon adják meg azokat. A fejlett ál weboldalak hamisított SSL-tanúsítvánnyal is rendelkezhetnek. Az ál weboldalak meglátogatását hamis üzenetekbe rejtett linkekkel érik el (pl. adatváltoztatási kérés a rendszeradminisztrátortól e-mailben, vagy jelszóváltoztatási kérés a banktól egy biztonsági incidenst követően, számlatartozás jelzése egy szolgáltatótól stb.). Ez különbözteti meg az eltérítéses adathalászattól, mivel itt a támadó az áldozata gépén nem módosít semmit sem.
- Kifigyelés (shoulder surfing): közvetlen megfigyelési technikát jelent, a támadó keresztülnéz a felhasználó vállán, hogy információt szerezhessen. A kifigyelés

zsúfolt helyeken hatékony, amikor a felhasználó begépeli a PIN-kódját egy ATM-nél (ennek észlelésére vannak az ATM-eken kis tükrök), vagy például nyilvános helyeken – internetkávézóban vagy könyvtárban begépeli ügyfél-biztonsági kódját, jelszavát stb.

- Szélhámosság (social engineering): a támadó a saját kilétéről megtéveszti a felhasználót, így érve azt el, hogy olyan információkat osszanak meg vele, amire egyébként nem lenne jogosult. Például a támadó rendészeti dolgozónak vagy rendszeradminisztrátornak adja ki magát, de nem ritka a kezdő munkatárs szindróma is, ami a kezdők felé megnyilvánuló segítőkészséggel él vissza.
- Adatszivárgás: Manapság mind a magánszemélyeknél, mind a szervezeteknél rengeteg elektronikus információ és adat keletkezik napi szinten. A kommunikációs csatornák és adathordozók lehetőséget adnak ezen adatok és információk felhasználók általi kezelésére és mozgatására. Adatszivárgásnak hívjuk azon eseményeket, amikor bizalmasnak/titkosnak (de semmiképp sem nyilvánosnak) minősített adatok a felhasználó vétlen vagy szándékos tevékenysége következtében kikerülnek a szervezet védett kontrollkörnyezetéből és fentiek miatt ezen bizalmas adatokhoz, információkhoz jogosulatlan hozzáférés történhet. Fontos a feltételes mód – történhet. Mivel az ily módon, a szervezet kontrollkörnyezetéből kikerült az adat vagy információ, a szervezetnek nincs lehetősége azt megvédeni, ergo úgy kell az ilyen adatokra tekinteni, mint potenciálisan kompromittálódott adatokra.
- Célzott támadás (APT - Advanced Persistent Threat): Az APT jellegű támadások jellemzője, hogy több, sokszor egymásra épülő támadási módszert is alkalmazva, lehetőleg minél észrevétlenebbül, akár hosszú ideig is rejtve, jellemzően nem ismert sérülékenységeket kihasználva támadják a célpontot, hogy ott kifejtsék tevékenységüket, ami lehet akár adatlopás, informatikai rendszerek megrongálása vagy más illegális tevékenység.
- A kiberbűnözés szó a kibertéren keresztül, számítógép-használat közben elkövethető jogellenes bűncselekményekre utal. Ilyenek lesznek például az adathalászat és a bankkártya adatok (név, szám, lejárat, cvc) ellopása online.

A **hackerek** olyan személyek, akik jól értenek a technikához, és képesek arra, hogy behatoljanak informatikai rendszerekbe és hálózatokba. Azok a hackerek, akik rossz szándékkal, rombolás, adatok törlése, ellopása vagy módosítása, általában véve haszonszerzés miatt törnek be, azokat fekete kalapos (black hat) hackereknek hívjuk. Vannak olyan fehér kalapos (white hat) hackerek, akiket hívunk még „Penetráció-

tesztelőknek" vagy „etikus hackereknek", ők az ügyfelek megbízásából, az ügyfél felhatalmazásával, a feltárt hibákat dokumentálva törnek be a rendszerekbe és a tapasztalataikat jelentés formában átadják az ügyfélnek.

"**Jelszótörés**". A jelszavak a mai napig az elsődleges hitelesítési adatai sok rendszernek. Egyetlen „faktor", amit az azonosítón kívül tudni kell a belépéséhez. Mivel azonban a jelszó ellopható, lefigyelhető, feltörhető, ezért kritikus rendszereknél már többfaktoros azonosítást, hitelesítést használnak. A jelszótörés [h] jelentése ennek megfelelően tehát a jelszó nyílt szöveges verziójának megszerzése. Több módszer is ismeretes erre (nyers erő, szótár alapú, szivárványtáblázat stb.) A nyers erő módszer használja fel a lehetséges jelszavak egymás utáni bevitelét a támadás kivitelezése során – ez kétségkívül lehet jelzője a jelszótörésnek, de nem lesz a célja. A jelszótörőnek ugyanis nem az a célkitűzése, hogy sok-sok jelszót próbálgasson, hanem az, hogy gyorsan találjon egy működőképeset a kiszemelt áldozatához. A szivárványtábla egy olyan táblázat, amiben a támadó előre kiszámolja és rögzíti számos különböző karaktersorozat kivonati értékét (hash), így ezeket a támadás során már nem kell kiszámolnia, hanem csak készen felhasználnia – a szivárványtáblával történő jelszótörés offline történik, a támadónak meg kell szereznie előzetesen a jelszó adatbázist. Fentiek miatt szükséges, hogy az informatikai rendszerek üzemeltetői különösen odafigyeljenek a jelszavak rendszerben történő kezelésére és védelmére, többek között a hibás bejelentkezések figyelésével és bizonyos számú próbálkozás utáni védelem (tiltás, felfüggesztés) életbe léptetésével, a jelszavak nem nyílt szövegként történő tárolásával és a jelszóadatbázisok fokozott védelmével.

Természetesen lehetnek olyan fenyegetések az adatokra, amelyekről nem tehet senki sem az adott kontextusban, így a „**vis maior**" kategóriába tartozik. Ilyen például az adatok esetében a tűz. Megfontolandó, hogy habár nem „vis maior", de mégiscsak potenciális fenyegetést jelentenek az adatokra az emberi tevékenységek a vétlen hibák, gondatlanság révén.

Minden egyes támadási formában közös, hogy az előnyeiket a felhasználók, tulajdonosok rovására akarják érvényesíteni és a Büntető Törvénykönyv (Btk) szerint ma már ezek számítógépes bűncselekményeknek számítanak.

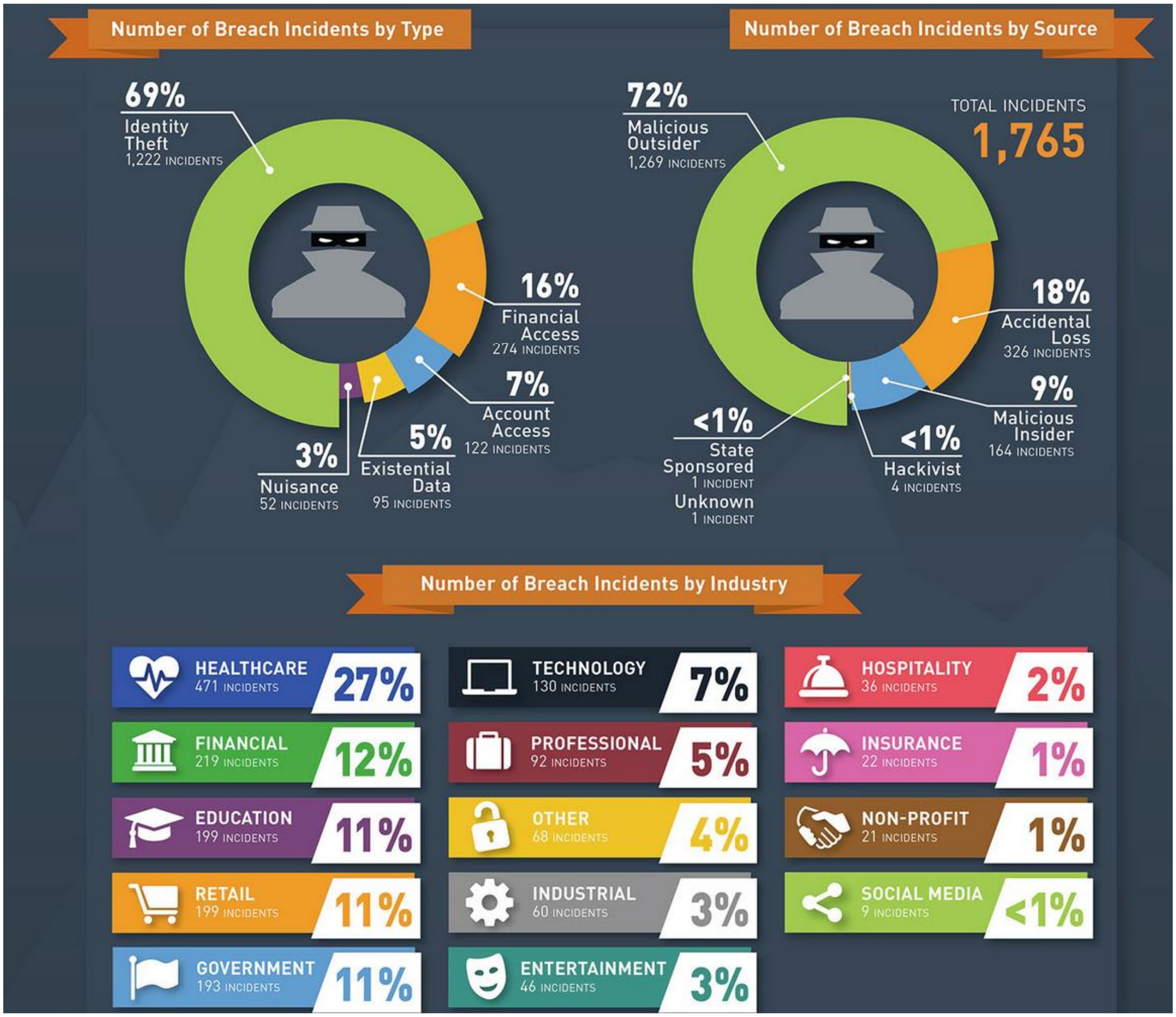
Sajnos a számítógépes bűnözés kifizetődő tevékenységnek tűnik. Elég csak a levélszemét küldéséből befolyó dollármilliárdokat megemlíteni, vagy az egyre emelkedő számú zsarolóvírus aktivitást, amelyből közvetlen bevétele származik a támadóknak, ha az áldozatok fizetnek. Ezen kívül sajnos megjelent a Fraud as a Service (FaaS), amely során

bárki hozzá nem értő is tud olyan internetes bűncselekményeket elkövetni, amelyhez korábban komoly programozói, informatikai vagy hacker tudás kellett. Például botnet hálózat bérlése, zsarolóvírus terjesztő hálózat bérlése, saját zsarolóvírus kampány készítése, kiválasztott célpontok támadása szolgáltatás megtagadásos (dDOS) támadással és még sorolhatnánk.

5 Fenyegetettségi és támadási trendek az elmúlt évekből

Számos internetbiztonsággal foglalkozó cég ad ki évről évre úgynevezett Internet Security Threat Report-ot [i]. Ezek a fenyegetettségi riportok bemutatják az addig tapasztalt és mért internetes fenyegetettségek statisztikáit. Természetesen, mint minden statisztika ez is egy bizonyos nézőpontot és eredményt mutat, ugyanakkor a trendek jól kiolvashatók belőlük. Jelen dokumentumban a Symantec, a világ egyik legjelentősebb információ- és informatikai biztonsági megoldásokat és szolgáltatásokat nyújtó cégének a 2017-es fenyegetettségi riportjából [i] mutatunk be pár fontosabb adatot. Fontos, hogy ezen adatok az egész világra kiterjedő információgyűjtő rendszerekből származnak.

5.1 Személyes adatokat érintő incidensek



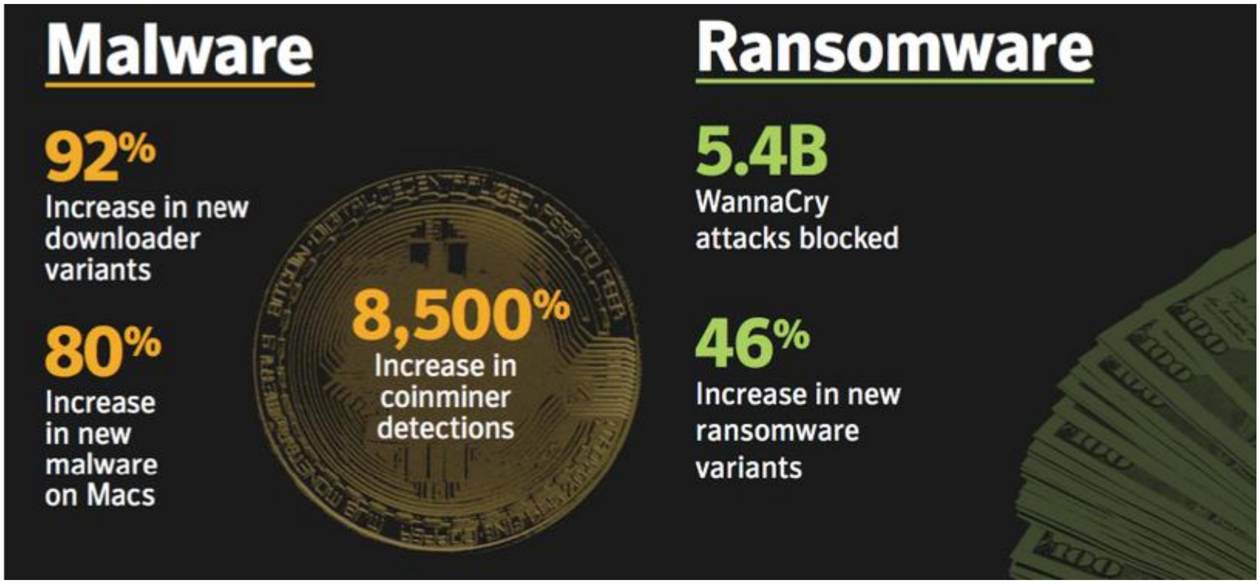
3. ábra Incidensek elemzése infografika. (https://breachlevelindex.com/assets/Breach-Level-Index-Infographic-2017-Gemalto-1500.jpg) [i]

Mint a statisztikából kiolvasható, az incidensek jelentős, mintegy 70%-ában személyes adatokkal történő visszaélés (Identity Theft – személyazonosság lopás) történt, de ha hozzáadjuk az ugyancsak személyes adatokat is tartalmazó Financial Access és Account Access kategóriákat, akkor már azt láthatjuk, hogy az incidensek 92%-ában személyes adatok is érintettek voltak.

Bár visszamenőleges adatok nem látszódnak, de aggasztó, hogy adatlopási incidensek listavezető szektora az Egészségügy. Az egészségügyi személyes adatok azért is

számítanak például a GDPR szerint is különleges személyes adatnak, mert egy bankkártyaszámot, vagy internetbenki hozzáférési jelszót pillanatok alatt le lehet tiltani, vagy meg lehet változtatni, az egészségügyi személyes adatok jelentős része nem változik. Hogy hol és milyen betegséggel kezeltek bennünket, milyen gyógyszereket szedtünk vagy szedünk a mai napig? Ezen adatok végigkísérnek minket életünk folyamán és ha egyszer nyilvánosságra kerültek, akkor lehetőséget adnak célzott személyes reklámokra, de extrém esetben konkrét támadások, vagy zsarolás alapjául is szolgálhatnak.

5.2 E-mail fenyegetettségek, kártékony programok, zsarolóvírusok



4. ábra, Kártékony programok és ezen belül a zsarolóvírusok számossága és aktivitása (2017 Internet Security Threat Report – Symantec) [i]

A világ e-mail forgalmának jelentős részét teszik ki a spam-ek, kéretlen levelek. Bár a Symantec statisztikája szerint az összes levélforgalom 55%-a spam (ez 2%-os emelkedés 2016-hoz képest), vannak olyan becslések, hogy ez az arány akár 80-90% is lehet valójában.

92%-kal nőtt azon programok száma tavalyhoz képest, amelyek célja alapvetően, hogy valamilyen kártevő programot töltsenek le a felhasználók eszközeire. Bár a korábbi években többek között azért is voltak népszerűek a Macintosh számítógépek, mert elenyésző számban voltak olyan kártevők, amelyek ezt a platformot támadták. Sajnos 2017-ben 80%-kal nőtt a kifejezetten Macintosh (fenti ábrán:Macs) számítógépeket támadó kártevők száma.

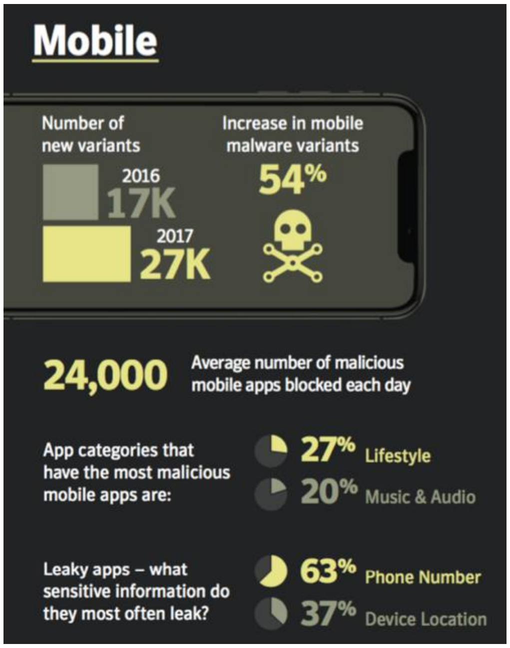
A zsarolóvírusok az elmúlt évek „slágertermékei”. A zsarolóvírus egyszerűen letitkosítja a gépünk/telefonunk fájljait és csak fizetés után, egy feloldókulcsot visszaküldve férhetünk hozzá újra a fájljainkhoz. Bár az első zsarolóvírust még floppylemezen küldözgették postán, manapság már milliós üzlet a támadóknak. A statisztikákból látszódik, hogy nem csak a darabszámuk, hanem a fajtáik és az általuk begyűjtött pénz is rohamosan növekszik, sajnos további ilyen támadásokra ösztönözve a bűnözőket.

2017 leghíresebb zsarolóvírus támadása az egész világot pár nap alatt végigfertőző WannaCry zsarolóvírus volt. Ez a fertőzés nem csak a globális kiterjedése miatt volt jelentős, hanem azért is, mert egy pár hónapja megismert, de milliónyi rendszeren még nem javított Windows sérülékenységen keresztül tudott terjedni és emiatt is számos olyan szolgáltatást érintett, amelyek a világon bárhol élő emberek mindennapjait érintették. A zsarolóvírus által letitkosított fájlok következtében jelentős zavarok és leállások voltak kórházakban, közlekedési rendszerekben, az államigazgatásban, a telekommunikációban, valamint oktatási- és pénzintézetekben is.

2017 során 5.4 Milliárd zsarolóvírus támadást blokkoltak világszerte. Ehhez a számhoz még hozzátartozik a sikeres fertőzések száma is sajnos, amelyről nincsen pontos számadat. Mindenesetre a zsarolóvírusok támadók általi népszerűségét mutatja, hogy 46%-kal nőtt az új zsarolóvírus variánsok száma az elmúlt évhez képest.

A zsarolóvírusok töretlen népszerűsége mellett megjelentek azon támadási próbálkozások, ahol csak fenyegetnek a támadók azzal, hogy ha nem fizet az áldozat akkor letitkosítják az eszközét. A támadók az ilyen esetekben bepróbálkoznak korábban ellopott jelszavak bemutatásával, amelyek ha véletlenül egyeznek az áldozat valamelyik használt jelszavával, akkor sokkal hatásosabb a fenyegetés. Ezért is fontos, hogy ne használjunk olyan jelszavakat, amelyek a világ leggyakoribb jelszavai közé tartoznak. A jelszavakról a 6.3.1 Hozzáférés-védelem, jelszavak, hitelesítés fejezetben olvasható bővebben.

5.3 Mobileszközök fenyegetettségei



5. ábra Mobileszközök fenyegetettségei (2017 Internet Security Threat Report – Symantec) [i]

Ahogy terjednek a mobileszközök – főleg az okostelefonokra és táblagépekre gondolva itt – úgy emelkedik a rájuk írt kártevőprogramok száma is. A 2016-os évhez képest tízezerrel, 54%-kal nőtt az új mobil eszközöket érintő kártevők száma. Naponta átlagban huszonnégyezer fertőzött mobil alkalmazás blokkolódik a védelmi programok által. Bár minden gyártó azt javasolja, hogy csak a hivatalos alkalmazás áruházból töltsünk le alkalmazásokat, természetesen lehetőség van ettől eltekinteni, bár ez jelentős kockázatokat hordoz magában. A hivatalos alkalmazás áruházakban is előfordulnak sajnos kártevőt tartalmazó alkalmazások, dacára annak, hogy az üzemeltetők igyekeznek mindent megtenni, hogy csak „tiszta” appok legyenek a felhasználók számára elérhetőek.

Rendkívül fontos, hogy az okoseszközöket is lássuk el megfelelő védelemmel, tartozzon bármelyik operációs rendszer kategóriába (Android, iOS, Windows, stb.).

Minden olyan neves gyártó, aki vírusvédelmi megoldásokat kínál, vagy valamelyik programcsomagja részeként, vagy önállóan, de kínál az okoseszközökre készített védelmi megoldásokat is. Általános szabály, hogy védelmi programokat is csak az adott platform hivatalos honlapjáról vagy applikáció boltjából töltsünk le (Google Play, Apple Store, Microsoft Store). Különösen ügyelni kell az okoseszközökön a számos ingyenes program által megjelenített reklámokra. Ezek gyakran ijesztgetik a felhasználókat azzal, hogy

vírusos az eszközük, és ezért azonnal töltsék le a felkínált vírusirtót. Nagyon gyakran pontosan ezek az ál-vírusirtó programok hordozzák a tényleges fenyegetettséget.

Mobileszközökre is elérhetőek olyan teljeskörű védelmi megoldások, amelyek képesek már ellopott/elveszett eszköz nyomon követesére, szülői felügyeleti funkciókra és minden olyan egyéb tevékenységre, amit az asztali PC – munkaállomás környezetben megszokhattunk. A vírusfenyegetettség annyira komoly, hogy már okoseszközökből is szerveztek az internetes bűnözök botneteket.[5]

Ha egy rosszindulatú program megfertőzte az eszközünket, akkor előforduhat, hogy a támadó vezérelni tudja a telefont távolról. Emelt díjas hívásokat indíthat, továbbküldheti a beérkező sms-eket, bekapcsolhatja a kamerát és a mikrofont és gyakorlatilag mindent megtehet az eszközzel, amit csak szeretne.

A mobileszközök esetében azonban nem csak a vírusfertőzés jelent problémát. A mobileszközeinket és a rajtuk tárolt adatainkat az eszközök mérete és hordozhatósága is veszélyeknek teszi ki. Minden esetben tegyünk az eszközre képernyő zárolást, amelyet csak PIN kóddal, jelkóddal, vagy valamilyen biometrikus azonostóval - jellemzően ujjlenyomattal oldhatunk fel. Így egy esetleges ellopás vagy elvesztés esetén nem fognak tudni a támadók az eszközünkbe belépni és ott jogosulatlan műveleteket végezni.

Az eszközeink fizikai védelme, az adatok védelme miatt is fontos. Lássuk el az eszközt telefont, tabletet olyan tokkal, amely gátolja a fizikai behatások káros következményeit. Tetessünk rájuk üvegfóliát, amely megvédi a kijelzőt a sérüléstől. Okostelefonok és tabletek esetében a kijelző különösen kritikus pontja az eszköznek, mert azon keresztül vezéreljük az eszközt. Ha sérül a kijelző – például mert élére ejtettük és összetört – akkor nem fogunk tudni utasításokat adni az eszköznek még akkor sem, ha számítógéphez csatlakoztatjuk és az eszköz maga működik. Ugyanis ilyenkor engedélyt kell adni, hogy a számítógép hozzáférjen az eszközhöz. De kijelző nélkül ez nem működik. Ilyenkor vagy kicseréltetjük a kijelzőt, vagy a teljes eszközt kicseréljük. Ilyenkor figyeljünk oda, hogy az adataink még az eszközön vannak és jó eséllyel el fognak veszni, hacsak nem volt mentésünk.

A másik fontos védelmi intézkedés a háttértárak titkosítása. Amennyiben például memóriakártyával van bővítve az eszközünk, egy ellopás vagy elvesztés esetén azt ki lehet venni az eszközből és más eszközben olvasható az adattartalma. Kivéve, hogyha titkosítottan tároltuk a rajta lévő adatokat. A háttértárak titkosítása egy opció, amelyet az eszköz biztonsági beállításai között találunk.

[5] **Például:** http://www.bbc.com/news/technology-37738823

A titkosítás megvéd az illetéktelen adathozzáférésektől, de nem véd meg az adatok elveszésétől. Sőt, ha a titkosító alkalmazás vagy a titkosító algoritmus nem jól működik, vagy sérül a titkosító kulcs, akkor sajnos mi sem fogjuk tudni az adatokat visszafejteni és abba helyzetbe kerülünk, mintha biztonságosan töröltük volna az adatainkat. Ezért rendkívül fontos az adatok rendszeres mentése. Erről a mentésekről szóló fejezetben szólunk bővebben.

Ha mobileszközök fenyegetettségeiről beszélünk, akkor nem mehetünk el szó nélkül a mobilalkalmazások hozzáférési igényei mellett sem. A mobilalkalmazások is hozzáférést igényelnek a telefon/tablet erőforrásaihoz. Az alkamazás célja és funkciója szerint ez a hozzáférés kiterjedhet akár a kamerára, mikrofonra, hiváslistára, geolokációs adatokra és még sorolhatnánk. Az alkalmazás használata során a felhasználási feltételekben a fejlesztők leírják, hogy az alkalmazáson keresztül milyen adatokat érnek el, és hogy mit tesznek ezekkel az adatokkal, kiknek adják át és milyen célból.

Érdemes ezeket figyelmesen elolvasni és ha egy alkalmazás túlzó jogosultságokat szeretne, vagy olyan adatokhoz szeretne hozzáférni, ami nem indokolt a funkcióját és célját tekintve, akkor keressünk másik, kisebb jogosultság igényű alkalmazást. Modernebb operációs rendszer verziókon már funkciónként adhatunk engedélyt az alkalmazásoknak az erőforrások elérésére. Az utóbbi évek tapasztalata, hogy rendkívül sok olyan adatbiztonsági incidens van, amely során mobilalkalmazások feljogosítva – vagy sajnos engdély nélkül - felhasználói adatokat továbbítottak a fejlesztőknek, akik ezen adatokat értékesítették vagy kiadták harmadik feleknek a felhasználók tudta és belegyezése nélkül.

Az alkalmazásfrissítések szintén hozhatnak igényt új funkciók elérésére. Automatikus frissítés esetén érdemes időnként átvizsgálnunk az alkalmazásaink jogosultságait, hogy történt-e negatív változás.

6 A védelem kialakítása

Az előző fejezet megmutatta, hogy az adatainkat láthatóan számos veszély fenyegeti. Ezek között vannak olyanok, amelyek bekövetkezési valószínűségét valamilyen védelmi intézkedéssel, kontrollal csökkenthetjük, és vannak olyanok, amelyek bekövetkezését nem láthatjuk előre és nem is tehetünk semmit a megtörténése ellen (földrengés, hurrikán, céltudatos betörő). Mindkét típusú fenyegetés következményeként az adatok, valamint az adattároló és a feldolgozó eszközök is megsérülhetnek, ellophatják őket, vagy

megsemmisülhetnek. Cél az, hogy ahol lehet, a fenyegetés megvalósulását megakadályozzuk, bekövetkezési valószínűségét csökkentsük. Ahol nem lehet vagy nem sikerült megakadályozni, ott pedig első lépésként felismerjük azt. Nagyon fontos célkitűzés lehet az is, hogy minden pillanatban legyünk képesek arra, hogy a bármilyen okból bekövetkezett információtechnológiai sérülés kárkövetkezményét gyorsan meg tudjuk szüntetni, vagy le tudjuk csökkenteni az elviselhető szintre. Ez csak akkor fog a gyakorlatban a kellő mértékben működni, ha megvannak az ehhez szükséges információk, így nem érheti ezeket semmilyen katasztrofális esemény sem. Ezért a védelmet nagyon gondosan kell kiépíteni.

A **biztonság mértéké**ben jelentős különbségek mutatkoznak abból a szempontból, hogy milyen kifinomult és mennyire automatizálható támadások ellen védett a rendszerünk.

Támadási szint / Támadó	Automata (program)	Ember	Védelmi szint
Kifinomult	-	+	magas
Programozott	+/-	+	közepes
Programokat lefuttató	+	+	alacsony

Kifinomult támadást kizárólag az ember képes végrehajtani, mivel ehhez a támadási cél minden összegyűjthető fizikai és logikai tulajdonságát intuitíven felhasználhatja a támadó. Az egyes támadási formákat programokba öntve számos bonyolultabb támadási forma is létrehozható, de ebben az esetben a program működésre bírásához a legtöbb esetben szakismeret is szükséges. Ezzel ellentétben a programokat lefuttató támadásoknál, ahol a támadónak csak az elindítógombot kell megnyomnia egy egyszerűen kivitelezhető támadás realizálható. Nyilvánvalóan mindhárom formához eltérő támadói tudásszint tartozik és némiképp eltérően is lehetséges védekezni ellenük. A védelemnek is növelnie kell a tudását az egyre hatékonyabb védelmi módszerek kialakításához, amiben nagyon fontos eszközök az automatizált támadások java része ellen védelmet nyújtó automatikus megoldások (tűzfal, vírusirtó, wifi-beállítások stb.). Az internet veszélyeinek egy részét úgy tudjuk kiszűrni, hogy nem engedjük meg a bejövetelét. Ebben segítenek az egyes tartalomellenőrző szoftverek, weboldalak elérését kategóriák alapján engedélyező vagy tiltó szoftverek, szülői felügyeleti szoftverek stb. A tartalomellenőrző szoftverek célja a weboldalakhoz való hozzáférés ellenőrzése és korlátozása, hogy csak olyan tartalmú oldalak jelenhessenek meg a számítógépünkön, amit szeretnénk, amit nem tartunk például károsnak a gyermekeink számára és aminek a megjelenítéséhez explicit módon – a

beállítások révén hozzá is járulunk. Ha korlátozni szeretnénk az interneten eltölthető időt, erre a szülői felügyeleti szoftverek alkalmasak.

Emlékezzünk a 2.1 fejezetben megadott definícióra: *a biztonság egy olyan kedvező állapot, amelynek megváltozását nem várjuk, de nem is tudjuk kizárni*. Annak elismerésével, hogy nincsen tökéletes (100%-os) biztonság, tudatában kell lennünk a 20%-os és a 80%-os biztonság közötti különbségnek, ami leggyakrabban a biztonsági incidensek számában mérhető. Másképpen fogalmazva,, magasabb szintű a biztonság, ha kevesebb a biztonsági incidens. A globális fenyegetettség állapotában nem bízhatunk abban, hogy védelem nélkül az informatikai rendszereink sokáig incidens nélkül maradnak. A biztonság tehát nem a „szükséges rossz”, hanem a folyamatok működőképességét biztosító eszköz.

Hogyan kell nekifogni a **biztonság megteremtéséhez**? Működőképes biztonságot teremteni az egyenszilárdság elvét figyelembe véve lehetséges, ami azt mondja ki, hogy úgy kell a védelmet kiépíteni, hogy minden eleme azonos erősségű legyen. Védelmi tekintetben ugyanis minden védelem olyan erős, amilyen erős a leggyengébb pontja. A támadó meg fogja keresni a védelem hiányosságait és a lehető legkevesebb ráfordítással a lehető legnagyobb eredményt akarja elérni, ez pedig a leggyengébben védett elem támadásával lehetséges legtöbb esetben. Ha ehhez hozzávesszük a biztonsági követelményeket, máris világos, hogy mit kell tennünk a biztonság érdekében: az általunk használt informatikai erőforrások (adatok/információk, technológiák, alkalmazások) biztonságáról – vagyis ezek bizalmasságáról, sértetlenségéről és rendelkezésre állásáról – kell a megfelelő mértékben gondoskodni.

Szervezeti keretek között a védelem szabályait Informatikai vagy Információbiztonsági Szabályzatban (IBSZ) szokták rögzíteni, amely követendő magatartásmintákat, előírásokat tartalmaz minden számítógép-felhasználó számára. Az IBSZ helye középen van a biztonsági előírások hierarchiájában, mivel felette a stratégiai szintű Információbiztonsági Politika, alatta pedig az operatív szintű eljárásrendek találhatók. A szabályzatok közé soroljuk még a katasztrófahelyzetben végrehajtható intézkedéseket tartalmazó Informatikai Katasztrófa-Elhárítási Terveket is. Ezek otthoni vetülete annak végiggondolása, hogy mit tehetünk az otthon tárolt adataink védelme érdekében a mindennapokban és extrém helyzetekben (pl. árvíz, lakástűz, betörés, adatvesztés megelőzése) is.

6.1 Felhasználók felelőssége az incidensek, biztonsági események során

A felhasználóknak kulcsszerepe van az információbiztonság fenntartásában, hiszen ők azok, akik nap, mint nap, ténylegesen hozzáférnek az adatokhoz, informatikai rendszerekhez. Ők azok, akik az adatokat előállítják, továbbítják, különböző informatikai eszközökön letárolják vagy adathordozókon hordozzák, majd az adatot megsemmisítik, ha ez szükséges. Fentiekből következően felhasználónak minősül mindenki, legyen vezető, üzemeltető, szakértő vagy külsős, aki hozzáfér a szervezet adataihoz. Otthoni környezetben ugyanez elmondható, hogy minden családtag, barát, rokon vagy ismerős, aki hozzáfér az otthoni informatikai rendszerekhez, az felhasználónak minősül.

A legfontosabb, hogy a felhasználók tisztában legyenek a fenyegetettségekkel, a szabályokkal, valamint azon folyamattal, hogy mit kell tenniük, hogy megelőzzék az információbiztonsági (és egyéb biztonsági) incidenseket, vagy ha megelőzni nem is sikerült, időben felismerjék azokat és tudják, hogy milyen csatornán lehet jelenteni azt az illetések felé.

A végfelhasználók hatalmas értéket képviselnek az incidenskezelést végző csoport vagy szervezet számára az incidenskezelés folyamatában. Ugyanakkor hatalmas felelősséggel is bírnak. Kritikus szerepük van az incidenskezelési folyamatban azáltal, hogy ők, a végfelhasználók az elsők, akik általában valamilyen incidens jelével először találkoznak. Gondolhatunk itt egy alkalmazás nem megszokott működésére, egy gyanús csatolmány beérkezésére az e-mail postafiókba, egy gyanús telefonhívásra, egy elhagyott pendrive-ra, ami az irodában a folyosón hever, vagy egy gyanúsan sétálgató ismeretlenre az irodában. Létfontosságú a szervezet számára a felhasználók azon képessége, hogy időben felismerjék a fenyegetettségeket és a megfelelő kockázati attitűddel felmérjék a valós veszélyt és időben jelezzék azt az incidensmenedzsmenttel foglalkozó szervezet számára.

6.2 A bizalmasság

Az üzleti életben értelemszerűen nagyon jelentős az üzleti titok védelme, ennek az az oka, hogy a vállalatok nagyon odafigyelnek az ügyfeleikre és az ügyfeleik adataira, és meg akarják előzni az ügyfelek adataival való visszaélést, valamint az ügyfeleik adatainak ellopását, hiszen ennek bekövetkezése súlyos bevétel-kiesést okozhat számukra, ahogyan ezt több példa is bizonyította a közelmúltban. 2018. május 25-től hatályos az Európai Unió Általános Adatvédelmi Rendelete (GDPR – General Data Protection Regulation), amely

minden olyan cégre és szervezetre, amely személyes adatokat kezel vonatkozni fog. A korábbi szabályokhoz képest némileg szigorodtak az elvárások. Ami jelentőset változott, az a büntetési tétel, ha az adatokért felelős szervezet nem tartja be a szabályokat, vagy ha emiatt az adatokat érintő incidens következik be.

Az adatokhoz való jogosulatlan hozzáférést alapesetben az akadályozza meg, ha valamilyen azonosítási és hitelesítési módszert használunk (például azonosító+jelszó). A jogosulatlan adat-hozzáférés ellen ezen túlmenően a titkosítás is védelmet nyújt. A kettő között az a különbség, hogy az azonosítás+hitelesítés jellegű hozzáférésvédelemnél a támadónak a védelem esetleges megkerülésével mégis sikerülhet hozzáférnie a védendő adatokhoz. Például megszerezve a jelszó kivonatokat /hash/, közvetlenül ezekkel fordul a hitelesítést végző rendszer felé, így nincs is szüksége az eredeti jelszavakra – ez az úgynevezett „pass the hash" támadás, Míg titkosítás alkalmazásával hiába fér hozzá a titkosított adatokhoz, azokat akkor sem tudja elolvasni a titkosító kulcs ismerete nélkül, vagy a feltörés megvalósítása nélkül. A titkosított adatok előnye az, hogy kulcs nélkül nem lehet az adatokat elolvasni. A titkosításnak azonban korlátja is van. Mivel kulcsot kell használnunk a titkosításhoz és a feloldáshoz is, ezért a titkosító kulcs elvesztésével nem tudunk többé titkosítani, a feloldáshoz szükséges kulcs elvesztésével pedig az adat használhatatlanná válik.

Azt az információbiztonsági tulajdonságot, amelyik biztosítja a tárolt adatok jogosulatlan hozzáférés vagy felfedés elleni védelmét, bizalmasságnak hívjuk. A jogosulatlan hozzáférés következményei lehetnek a sértetlenség (benne a hitelesség) és a rendelkezésre állás sérülése is, amennyiben a támadó átírja az egyes adatokat vagy törli azokat. Az adatok jogosulatlan módosítása elleni védelmet tehát a bizalmasság információbiztonsági jellemző biztosítja, a sértetlenség csupán detektálni képes ennek megváltozását, de nem tudja megakadályozni azt.

Bizalmasságról akkor beszélhetünk, ha az adataink egy részének megismerhetőségét korlátozzuk, és minden időpillanatban tudjuk, hogy ki van feljogosítva az egyes adatokhoz történő hozzáférésre. A bizalmasság megteremtését lehetséges saját és felhő környezetben is értelmezni. Amennyiben a saját gépeinken és egyre több esetben a felhő szolgáltatásokban tárolt adatokról van szó, lehetőségünk van hozzáférés-védelmet kialakítani (többször használható jelszó, erősebb esetekben valamilyen egyszer használatos jelszó (SMS kód, percenként változó token kód) vagy tanúsítvány). Ez annyira védi az adatainkat, amennyire a védelmet nem lehet megkerülni. Vagyis ez a védelem nem sokat ér akkor, ha a támadó meg tudja kerülni a hozzáférés-védelmünket (például

rendszerszinten tevékenykedő kártékony kód használatával szerez hozzáférést minden helyi adatunkhoz anélkül, hogy bármilyen jelszó ismeretére szüksége lenne).

Ettől erősebb védelmet biztosítanak a különböző titkosító programok, melyeket használhatunk lemezpartíciók, USB-lemezek, adatbázisok, fájlok, tömörített állományok és kimenő üzenetek titkosítására is. Ekkor a megfelelő kulcs nélkül nem lehetséges elolvasni a titkosított adatokat még akkor sem, ha a támadó megszerezné a titkosított fájlokat. Ez a védelem persze nagymértékben függ az alkalmazott kriptográfiai algoritmustól és a kulcs hosszúságától. Önmagában nem elegendő a titkosítás megléte, az is szükséges, hogy megfelelően legyen az adat titkosítva. Ehhez nélkülözhetetlen, hogy ismerjük az egyes algoritmusok tulajdonságait olyan szinten, hogy meg tudjuk állapítani az alkalmazott paraméterek megfelelőségét. Felhasználói szinten már egy alapszintű titkosítás is megfelelő védelmet nyújthat, mivel a védett adatok értéke várhatóan nem áll arányban azzal az erőforrás szükséglettel, ami az adatok ellopásához és feltöréséhez szükségesek. Konkrétan egy hacker nem fogja célzottan az idejét pazarolni arra, hogy az otthoni titkosítással védett családi költségvetést tartalmazó excel táblát vagy fotóalbumot feltörje. Vagy ha el is lopja egy tolvaj a hordozható adattárolónkat (pendrive, mobil merevlemez), sok esetben nem lesz elegendő tudása és motivációja ahhoz, hogy a rajta lévő titkosított word fájlokat feltörje – amelyek például a szakdolgozatunk anyagait tartalmazzák. Az adataink bizalmassága így megmaradhat az adathordozó eltulajdonítását követően is.

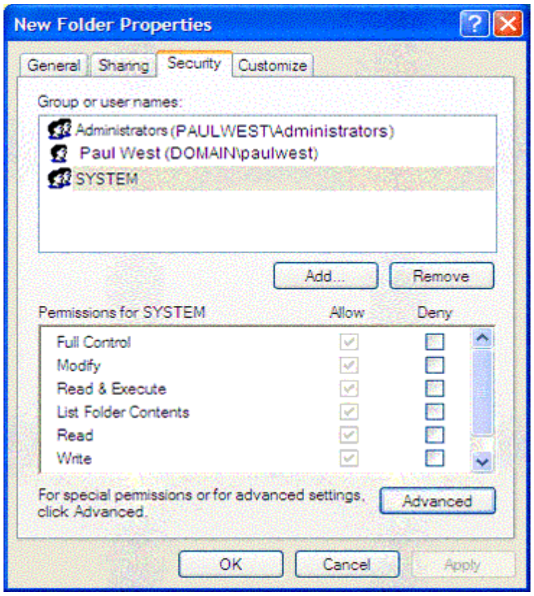
6.2.1 Bizalmasság az operációs rendszerben

Az operációs rendszerek biztonsága, felhasználói szemszögből nézve, tipikusan fájlok biztonságát jelenti. A fájlok biztonságáról több aspektusból lehet beszélni, a hozzájuk kapcsolódó műveletek révén. Ezek az olvasás, írás, törlés, módosítás. Fontos kérdés, hogy ki rendelkezik ezekkel a **fájl-jogosultságok**kal?

Az olvasást megakadályozza a titkosító program általi **fájl-titkosítás** – amikor esetleg ugyan megnyithatjuk a fájlt, de értelmezni nem tudjuk - vagy a szövegszerkesztőben való megnyitás jelszóhoz való kötése is, amikor a jelszó ismerete nélkül itt sem tudjuk megnyitni (**feloldani a titkosítást**) a fájlt. Jelszavas védelmet beállíthatunk irodai programcsomagok által készített dokumentumokhoz (szöveg, táblázat, prezentáció stb.) vagy tömörített fájlokhoz egyaránt (zip, rar stb.). A biztonságkritikus fájlokhoz (pl. digitális aláíráshoz használható kulcs) a rendszer nem is engedi meg a jelszó nélküli hozzáférést alapértelmezésben.

A fájlt akkor tudjuk kiírni egy háttértárolóra, ha ahhoz van jogosultságunk, egyébként a létrehozni kívánt fájl a memóriából nem megy tovább és onnan a program bezárásakor (ha jól van a program memória kezelése megírva) törlődik. Egy fájlba beleírni (módosítani) akkor lehetséges, ha az a fájl módosításra – írásra – hozzá van rendelve a felhasználóhoz, egyébként nem fogja tudni a felhasználó a módosításokat elmenteni. Fontos megemlíteni azt is, hogy van-e olyan eleme egy fájlnak, amit a rosszindulatú támadás során fel lehet arra használni, hogy a tulajdonos tudta nélkül írjanak bele a fájlba vagy a rendszerbe – ilyenek lehetnek például a makrók [j].

Otthoni számítógép használat esetén javasolt minden családtagnak saját felhasználói fiókot létrehozni általános jogosultsági szinttel. Az adminisztrátori fiókot pedig csak akkor használni, ha feltétlenül szükséges. Ezzel lehetővé válik, hogy az operációs rendszerünkben korlátozzuk az egymás adataihoz való hozzáférést.



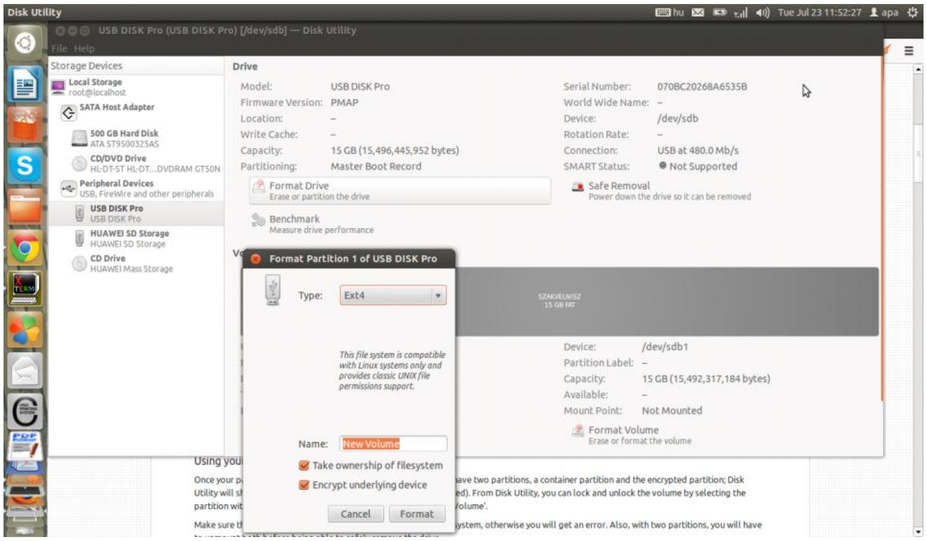
6. ábra Hozzáférések megadása Windows operációs rendszerben

6.2.2 Merevlemezek és USB-lemezek titkosítása

Az adataink mindazok számára alapértelmezett esetben hozzáférhetők, akik a tárolására szolgáló lemezek (belső, külső, felhő, USB) birtokában vannak. Leggyakrabban a jogos tulajdonosa van birtokon belül, de a támadók sokszor sikeresen tudják ezeket a tárolókat – illetve a rajtuk tárolt adatokat távolról – eltulajdonítani. Voltak, vannak és lesznek hordozható számítógép-lopások és távolról betörni kívánó tolvajok is. Emiatt is szükséges, hogy védjük adatainkat.

Az adatok bizalmasságának legáltalánosabb védelmére a titkosítást használják. Lehetséges titkosítani mind a számítógépek merevlemezét, mind pedig egy külsőleg csatlakoztatható USB-eszközt is, illetve egyedileg fájlokat vagy könyvtárakat. Egy lényeges különbség létezik rendszerindításra alkalmas és nem alkalmas lemezek titkosítása között, mégpedig az, hogy a rendszerindításra alkalmas lemeznek kell, hogy legyen egy nem titkosított része is, ahonnan a rendszer addig betölthető, amivel már a titkosított partíciót el tudjuk érni. Rendszerindításra nem felkészített lemez teljes mértékben titkosítható.

A titkosítás előnye az, hogy nem kell aggódnunk innentől kezdve az adatok miatt, ha esetleg az eszközt el is lopnák, amennyiben a jelszót megfelelően erősre választottuk, az alkalmazott megfelelően erős kriptográfiai titkosítás visszafejtése jellemzően meghaladja a támadók erőforrás-lehetőségeit. Természetesen itt is vigyáznunk kell a jelszó rendelkezésre állásának megmaradására, mert enélkül a titkosított adatok előlünk is el lesznek rejtve mindörökre.

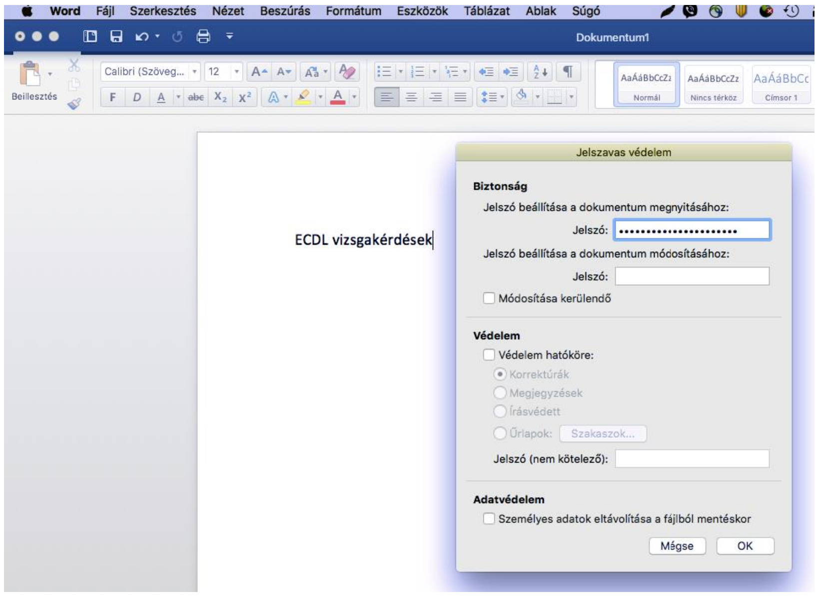


7. ábra USB-lemez titkosítása Linuxon

6.2.3 Titkosítás irodai programcsomagokban

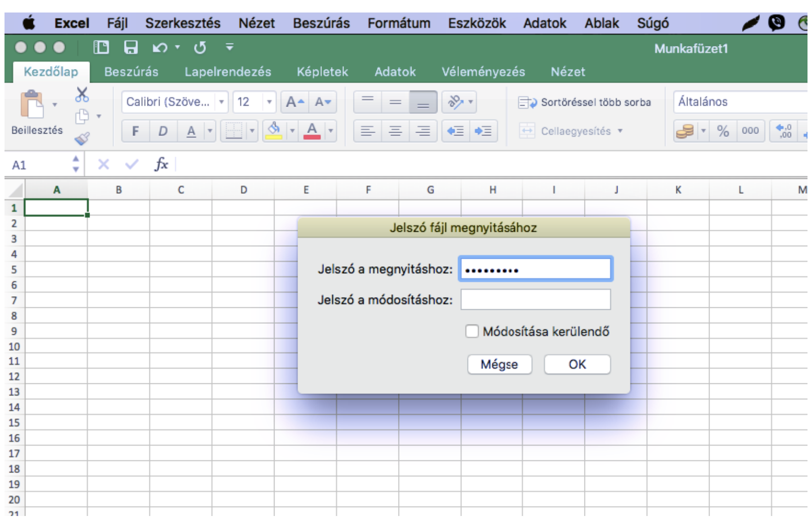
A szövegszerkesztők, táblázatkezelők, irodai programcsomagokban használható programok beépített funkciókat tartalmaznak a szöveg jelszavas védelmének megteremtéséhez, más szóval a **dokumentumtitkosítás**hoz. Amennyiben használjuk ezt a funkciót, a szövegszerkesztő bekér tőlünk egy – megfelelően biztonságos – jelszót, aminek segítségével a teljes dokumentumot titkosítja, így azt a jelszót nem ismerő számára

teljesen olvashatatlanná teszi. Vigyázat, amennyiben a jelszót elfelejtjük, nem biztos, hogy létezik olyan módszer, ami vissza tudja állítani az eredeti tartalmat! A nem megfelelő titkosítás tehát az adataink számunkra való hozzáférhetetlenségét is eredményezheti, amivel túllőhetünk az eredeti titkosítási célkitűzésen.



8. ábra Megnyitási jelszó beállítása Mac Microsoft Word 2016 szövegszerkesztőben

Mac Microsoft Word 2016 programban az Eszközök / Dokumentumvédelem menüpontra történő kattintással jelenik meg a jelszót bekérő ablak



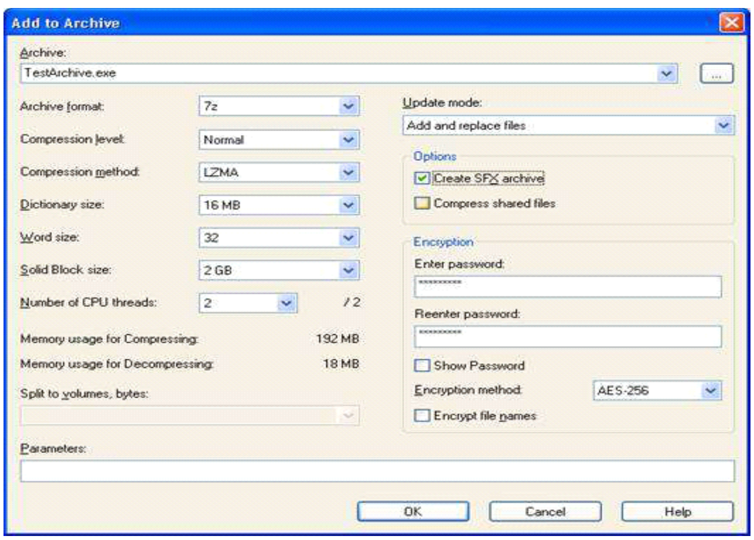
9. ábra Megnyitási jelszó beállítása Mac Microsoft Excel 2016 szövegszerkesztőben

A képen látható Mac Microsoft Excel 2016 verzióban a File menü / Jelszavak menüpontra történő kattintással jelenik meg a jelszót bekérő ablak.

Nem lehet elégszer elismételni, hogy a biztonság kulcsa ezekben az esetekben is a jelszó megfelelő megválasztása, hiszen egy gyenge jelszóval a védelem pillanatok alatt feltörhető.

6.2.4 Bizalmasság tömörített állományoknál

A tömörítőprogramok legtöbbje fel van arra készítve, hogy a tömörített állományokat olyan titkosítással védjék, mely a felhasználó által megadott jelszó/jelmondat alapján végzi el a fájl kriptográfiai titkosítását. A titkosítást az archívum létrehozásakor kell kiválasztani és a jelszót beállítani a **fájltömörítés**hez, az alábbi kép jobboldalán találhatunk ehhez segítséget.



10. ábra Jelszó beállítása archív állomány létrehozásakor

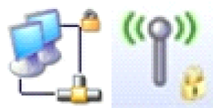
A megfelelő jelszó kiválasztása itt sem árt, mivel egy jelszótörő programmal rendelkező támadónak egy 10-számjegyből álló, vagy egy egyszerű (pl. csak az angol ábécé kisbetűiből álló) jelszó megfejtéséhez kb. 30 másodpercre van szüksége, egy közepesen erős számítógépen.

6.3 Hálózat és bizalmasság

A nyílt internetes kommunikáció során nemcsak a jogosultak láthatnak bele az adatokba. Adatok alatt egyrészről a hálózaton továbbított adatfolyamot, másrészről a hálózaton elérhető eszközökön tárolt adatokat – összefoglaló néven a **hálózati adat**okat értjük. A támadók a hozzáférés-védelmi rendszerek és a protokollok gyengeségeit, a ki nem javított programhibákat, valamint a felhasználók jóhiszeműségét kihasználva számtalan esetben képesek megszerezni jogosulatlanul az adatainkat és többször sikeresen vissza is élnek vele. Ma már sajnos számos támadás ismert, ami a kommunikációs hiányosságokra, és a felhasználók megtévesztésére alapozza sikerét. Fontos az adathalászat fogalmával megismerkedni, és a támadók sokszor felhasználják létező cégek, személyek neveit is a bizalom felkeltése érdekében. Ennek során alkalmanként és ideiglenesen hamis weboldalakat is felhasználhatnak, amelyek a megtévesztésig hasonlítanak az eredetihez. A hamis weboldalak segítségével a támadók kicsalhatják az eredeti honlapon megadni kívánt azonosítási és egyéb adatokat (ügyfélszám, felhasználói név, jelszó, egyéb személyes adatok, akár bankkártya adatok is). A hazai bankok mindegyike biztonsági tanácsokat és ajánlásokat fogalmaz meg a felhasználók számára, a biztonság érdekében. A szabályok kikényszerítését otthoni felhasználók esetében egyrészt tűzfal programok (personal firewall) végzik, másrészt választhat a felhasználó olyan komplex internet védelmi csomagot is, amely tartalmaz beépített tűzfalat, behatolás detektálót, spam és vírusszűrőt, szülői felügyelet programot, illetve akár az internet bankolás során védő böngésző modulokat is. Akár külön-külön, akár csomagban veszi meg a felhasználó, a lényeg, hogy otthoni környezetben is legyenek védettek az eszközök. Ugyanez vonatkozik természetesen az okostelefonokra is, mint funkcionalitásban ma már a személyi számítógépekkel vetekedő eszközök.

A hálózatokon belül megkülönböztetünk védett és nem védett hálózatokat. A védett hálózatok tulajdonsága, hogy valamilyen korlátozást alkalmaz a hozzáféréshez, és csak az arra feljogosítottaknak engedi meg a hálózati kommunikáció során a rendszerekhez való hozzáférést és az adatok olvasását és küldését.

A csatlakoztatható védett vezetékes hálózatot az első, a védett vezeték nélküli hálózatot pedig a második ikon jelöli.



11. ábra Védett hálózati csatlakozások megjelenítése

A hálózatra való csatlakozásnak a leggyakoribb biztonsági kihatása egyszerűen szólva az, hogy megfertőződhet a számítógép és okostelefon, de akár okoseszköz is rosszindulatú szoftverekkel. A hálózatra történő csatlakozás biztonsági vonatkozása ennél fogva a személyes és privát adatok védelme köré csoportosul, hiszen a netre kötött gépeken tárolt adatokhoz a külső támadó egy sikeres támadás során korlátozás nélkül hozzáférhet, illetőleg tetszés szerint használhatja a számítógépet és annak erőforrásait.

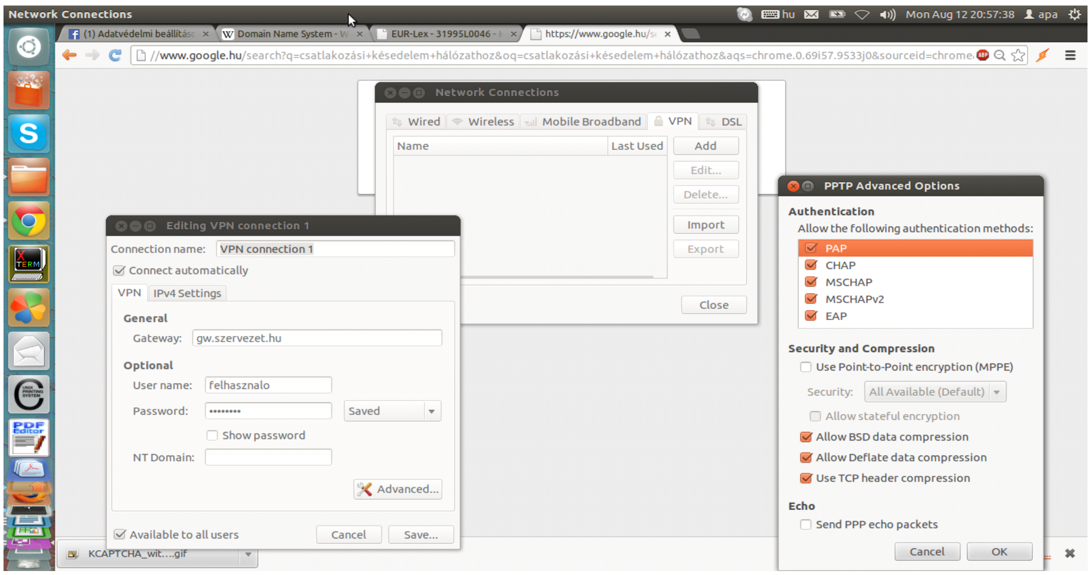
Gyakran felhasználják bejegyzett cégek neveit a személyes biztonsági adatok megszerzéséhez az eltérítéses adathalászat során. A támadó módosítja áldozata számítógépén például az internetes bankjának a címét, Így az áldozat azt hiszi, hogy annak adta meg az adatait, akit lát, nem gondol támadásra.

6.3.1 Hozzáférés-védelem, jelszavak, hitelesítés

A támadások legtöbbjét hálózaton keresztül követik el abból az egyszerű okból kifolyólag, hogy egy internetre kötött számítógépet, okoseszközt és okostelefont az egész internetközössége lát, míg egy számítógép esetén, a számítógépet tartalmazó helyiségbe, otthoni gépek esetén a lakásunkba fizikailag belépők száma igen erősen korlátozott szokott lenni. Míg korábban a hálózatok logikai védelme (tűzfal, tartalomszűrő, adatszivárgás-elleni védelem) sokkal nagyobb jelentőségű volt, mint a fizikai védelem, manapság a hordozható eszközök korában az eszközök fizikai védelmére is komoly figyelmet kell fordítani. Egy telefont könnyű elveszíteni, könnyen kikaphatják az ember kezéből egy forgalmas helyen. A hordozható eszközök, laptopok túlnyomó többségét autókból lopják ki. Ezért a legrövidebb ideig sem szabad autóban őrizetlenül hordozható eszközt hagyni, még zárt helyen, például csomagtartóban sem. A városok forgalmas helyein (áruházak, plázák, parkok, iskolák) kifigyelik a tolvajok, hogy ki pakol laptopnak tűnő táskát csomagtartóba, és vagy ott helyben, vagy a következő parkolásnál ellopják azt. Mire a tulajdonos visszatér, az eszköznek hűlt helye lesz. Sokszor a tulajdonos még azt sem tudja, hogy honnan lophatták el az eszközt. Ilyen esetekre jótanács az, hogy legyen titkosított a háttértár, az

eszköz legyen védve jelszóval, a telefonon is legyen képernyőzár, a SIM kártyán pedig PIN kód. Nem utolsó sorban ne tároljunk nem mentett adatokat a hordozható eszközeinken, hiszen telefont tudunk venni másikat, de például a gyermekünk első lépéseit megörökítő videót soha többé nem vehetjük fel újra.

A VPN (Virtual Private Network – Virtuális Magánhálózat, melyekről a 3.3 Számítógép-hálózatok fejezetben szóltunk korábban) kialakításához is kell egy olyan szoftver, amely a két végpontot titkosított csatornán összeköti és ahol azonosítás és hitelesítés történik, meggyőződve arról, hogy valóban a jogosult személy jelentkezik be. Ezt mutatja a következő ábra.



12. ábra Bejelentkezés VPN hálózatba

Általában minden hálózatnál van valaki, aki kiosztja és visszavonja a fájl- és eszköz-hozzáféréseket – ha egynél több személynek kell hozzáférést adni a saját zárt hálózatunkhoz, ezáltal megvalósítottunk egy **hálózati adminisztrátor**i szerepkört, aki a hálózaton belüli hitelesítés, feljogosítás és számonkérés kezelésére van feljogosítva, és feladata fenntartani a szükséges adathozzáférést a hálózaton. Otthoni környezetben ez jellemzően az otthoni vezeték nélküli hálózatunkhoz való hozzáférést jelenti. Célszerű első lépésként megváltoztatni az alapértelmezett adminisztrátori (admin) jelszót, majd beállítani hozzáférési jelszót (wifi jelszót), mivel a rádiójelek nem állnak meg a falnál és nem feltétlenül jó, ha a szomszéd a mi vezeték nélküli hálózatunkon keresztül internetezik.

A hálózat biztonságát számos veszély fenyegeti. Tudatában kell lenni annak, hogy a nem védett vezeték nélküli hálózat használata lehetővé teszi az adataink megismerését a

forgalmat lehallgatók számára, vagy az adatok szivárogtatásánál ezt a jogosultak követik el, akár a tudtuk nélkül is. A jelszavas védelem kialakításánál nagyon fontos, hogy a jelszó megfelelően biztonságos legyen. A jó jelszókezelés szabályait ajánlott betartani, mint a jelszavak másokkal való nem megosztása, időszakos megváltoztatása, megfelelő jelszó-hossz, megfelelő jelszó-karakterek – betűk, számok és speciális karakterek – együttes használata, valamint, hogy a jelszavakat ne írjuk fel füzetbe, excel fájlokba, cetlikre és ne használjuk ugyanazt a jelszót több helyen.

A jelszavak használatakor három típusú jelszót különbözetünk meg:

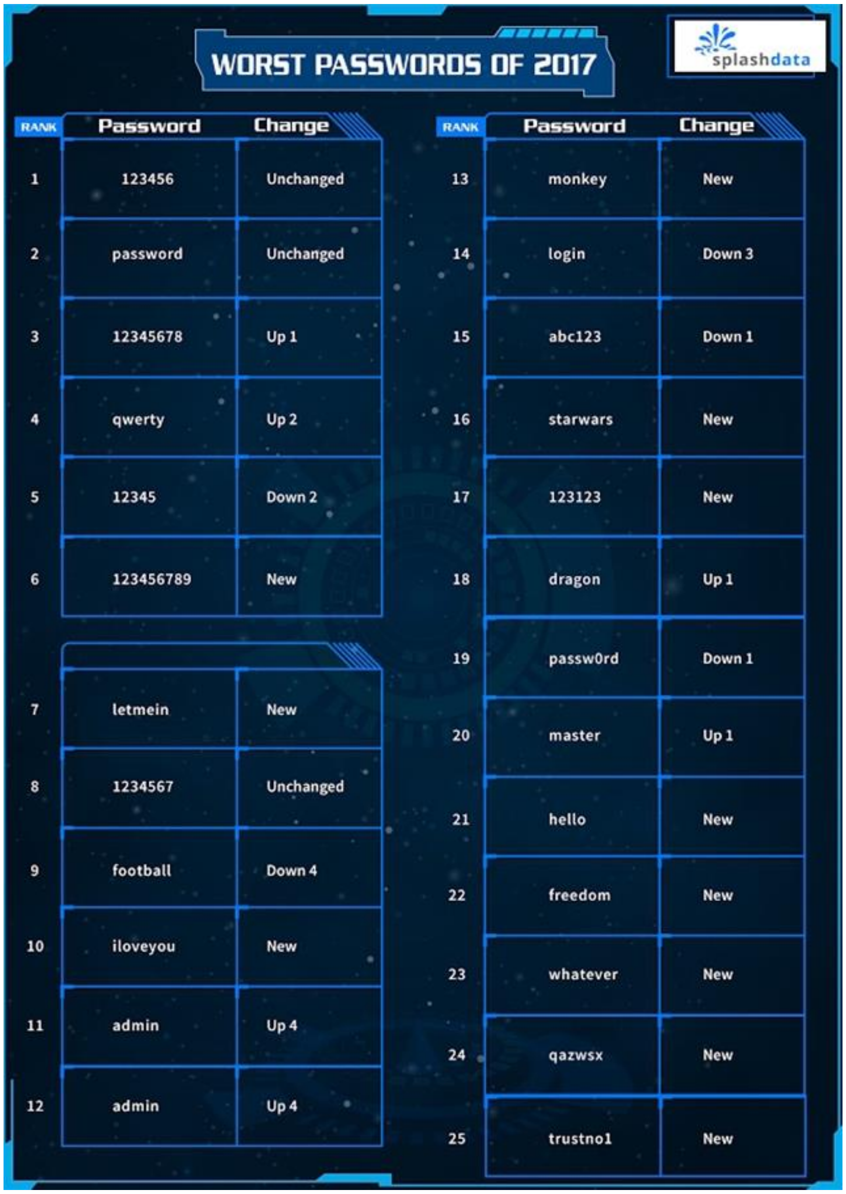
- többször használatos jelszó: egyszer megadjuk adott rendszerben, majd a következő jelszóváltoztatásig ezt a jelszót használjuk.
- egyszer használatos jelszó (OTP – one time password): ezt a jelszót vagy a felhasználó saját maga generálja és a generálás után csupán egyetlen egyszer használhatja fel – jellemzően egy token, hardveres eszköz szükséges hozzá, vagy azon rendszer állítja elő, ahová belépni szándékozunk és valamilyen csatornán eljuttatja hozzánk. Ennek legékesebb példája a bankok internetbankolás során alkalmazott belépési SMS jelszava, illetve tranzakció hitelesítő SMS jelszava.
- biometriai jelszó: az ember valamely fiziológiai jellemzője (pl. ujjlenyomat, hang, retina, tenyérlenyomat stb.)

A rossz jelszavak nem nyújtanak biztonságot, hiszen a potenciális támadót nem tudják megállítani, legfeljebb egy-két pillanattal késleltetni tudják a támadás bekövetkezését, mert a rossz jelszavak feltörését vagy kitalálását másodpercek alatt el lehet végezni. A jelszóhasználati rossz szokások bemutatására számos elemzés készült itthon és a nagyvilágban is.

Mit is jelent a megfelelően erős, megfelelően biztonságos jelszó? A jelszóerőssége három dologtól függ alapvetően. A jelszó kódolását végző algoritmustól (erre általában a felhasználónak nem sok ráhatása van), a jelszó hosszától (ez már függhet a felhasználótól, bár egyes helyeken meghatározzák, hogy milyen hosszú (például 8-15 karakterig terjedő) jelszót választhatunk és végül a jelszó bonyolultságától. Az általános ajánlás a jelszóválasztással kapcsolatban az, hogy ne legyen könnyen kitalálható, a felhasználóra utaló (pl. születési év, lakcím, házikedvenc neve stb.), illetve ne legyen a jelen dokumentumban is bemutatott legjellemzőbben használt jelszavak között (például 123456 – sajnos ezen jelszó továbbra is a legrosszabb jelszavak listájának éllovasa). De hogy milyen is legyen? Legyen legalább 8-15 karakter hosszú, tartalmazzon kis és nagybetűket, számokat és egyéb karaktereket. Ha nincs a hossz korlátozva, akkor érdemes több jelszót

egymás mögé fűzni, illetve léteznek olyan jelszószéf alkalmazások is, amelyek képesek előre megadott feltételek mentén jelszavakat generálni számunkra – ezekről később még lesz szó. Még egy fontos dolog, hogy a jelszavainkat ne tároljuk nyílt szöveges állományként (pl. egy excel táblában, vagy papírra leírva a gépünk mellett.) Ha lehetséges ugyanazt a jelszót ne használjuk egynél több alkalmazásban.

2018 májusában többszázezer, magyar felhasználók által használt jelszó is kikerült az Internetre, ezekből egyelőre még nem készült nyilvánosan elérhető statisztika. Ezért most egy angol nyelvterületre vonatkozó „legrosszabb 25 jelszó" statisztikát mutatunk be. Ez az elemzés is a felhasználók által használt, többször használatos jelszavakra vonatkozik, de a korábbi események megmutatták, hogy a jelszóképzés terén nincs olyan nagy különbség a világ számítástechnikai felhasználói között, ezért például a „jelszo" jelszó igen gyakori lehet Magyarországon is. Amennyiben a lenti táblázatban szerepel a jelszavunk, vagy nagyon hasonlít rá, akkor sürgősen változtassuk meg, figyelembe véve az előző bekezdésben szereplő tanácsokat.


WORST PASSWORDS OF 2017

splashdata

RANK	Password	Change
1	123456	Unchanged
2	password	Unchanged
3	12345678	Up 1
4	qwerty	Up 2
5	12345	Down 2
6	123456789	New
7	letmein	New
8	1234567	Unchanged
9	football	Down 4
10	iloveyou	New
11	admin	Up 4
12	admin	Up 4
13	monkey	New
14	login	Down 3
15	abc123	Down 1
16	starwars	New
17	123123	New
18	dragon	Up 1
19	passw0rd	Down 1
20	master	Up 1
21	hello	New
22	freedom	New
23	whatever	New
24	qazwsx	New
25	trustno1	New

13. ábra 25 leggyakrabban használt jelszó 2017-ben (forrás: SplashData) angol nyelvterületen

A biometriai védelem viszonylag ritka otthoni felhasználásban, de a kritikus biztonságú helyszíneken alapértelmezett a használatuk. Ilyen védelmi technika az ujjlenyomat, kézgeometria, tenyérlenyomat beolvasása, hangazonosítás vagy retina-szkenner a hozzáférés-védelemben.

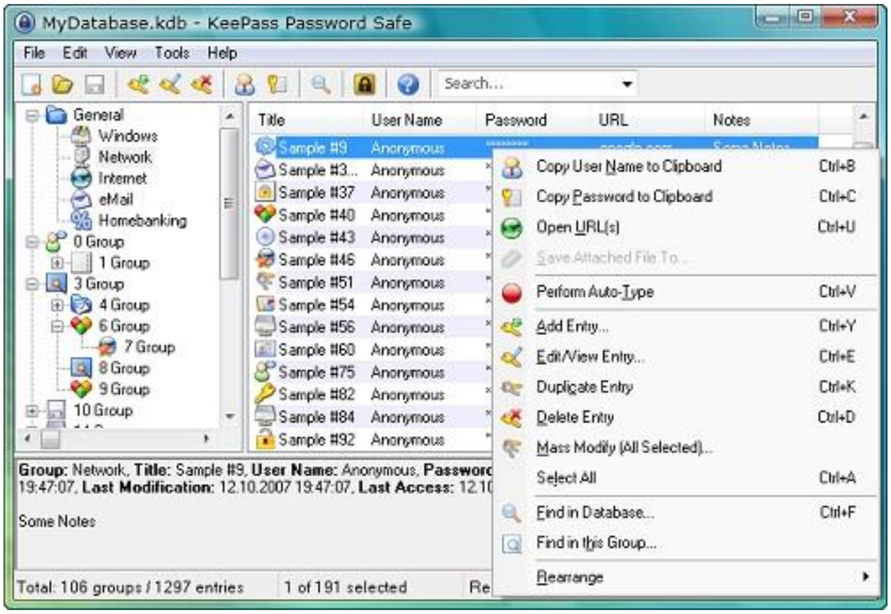
Az eszközök fizikai biztonságának növelésére használható módszer például hordozható számítógépek esetén a biztonsági kábelek (Pl. Kensington lock) alkalmazása, hogy a támadó ne tudja egyszerűen ellopni az eszközöket, fizikailag legyen meggátolva benne.

A fizikai védelem témakörébe tartozik valamelyest a webkamerák védelme is. A számítógépekhez kapcsolt vagy beépített webkamerákat egy külső támadó a saját irányítása alá tudja vonni bizonyos támadásokkal - még akkor is, ha nem világít a webkamera működését jelző LED, így erősen javasoljuk a webkamerák „megvakítását" használaton kívül (pl. egy ragasztócsíkkal való leragasztását vagy egy papírdarabbal való lefedését).

6.3.1.1 Jelszószéf

A jelszószéfek olyan alkalmazások, amelyek egy titkosított adatállományban eltárolják a felhasználók által alkalmazott jelszavakat és a hozzájuk kapcsolódó egyéb információkat (kapcsolódó weboldal, vagy alkalmazás, felhasználónév, jelszólejárat, megjegyzés). A jelszószéf alkalmazásánál két dologra kell figyelni. Az első, hogy a széfet nyitó mesterjelszó (Master Password) kellően biztonságos legyen és ne felejtsük el. Mert ebben az esetben mi sem fogunk hozzáférni a jelszavainkhoz. A másik fontos dolog, hogy legyen a titkosított adatokat tároló fájlról mentésünk. Mert ha a fájl megsérül, vagy törlődik – vagy neadjisten egy zsarolóvírus letitkosítja, akkor szintén nem fogunk tudni hozzáférni.

Az egyik legnépszerűbb és ingyenes ilyen alkalmazás a KeePass alkalmazás. Erős titkosítással védi a beleírt adatokat, képes előre megadott szempontok szerint jelszavakat generálni nekünk, illetve logikus tárolási struktúrát ad és nem utolsósorban tartalmaz egy jelszóerősség mérőt is, amely útmutató lehet a felhasználónak. Egy rendkívül hasznos tulajdonsága, hogy ha az alkalmazásból másoljuk ki az adott jelszót (Copy Password to Clipboard), akkor az 12 másodpercen belül törlődik a vágólapról, meggátolva más alkalmazás hozzáférését.



14. ábra KeePass Jelszószéf

Munkahelyi környezetben érdemes megérdeklődni az információvédelemmel kapcsolatos területtől, hogy mi a céges szabály az ilyen jelszószéf alkalmazásokkal kapcsolatban, mert ha nincs valamilyen központi menedzsment, akkor pont az ellenkezőjét is elérhetjük az eredeti célnak és akár üzletmenetfolytonossági incidenst is okozhatunk, ha senki nem fér hozzá egy fájlhoz vagy alkalmazáshoz, csak azért mert egy ilyen széfben tároltuk a jelszavakat. Fentiek miatt elsősorban otthoni használatra javasolt.

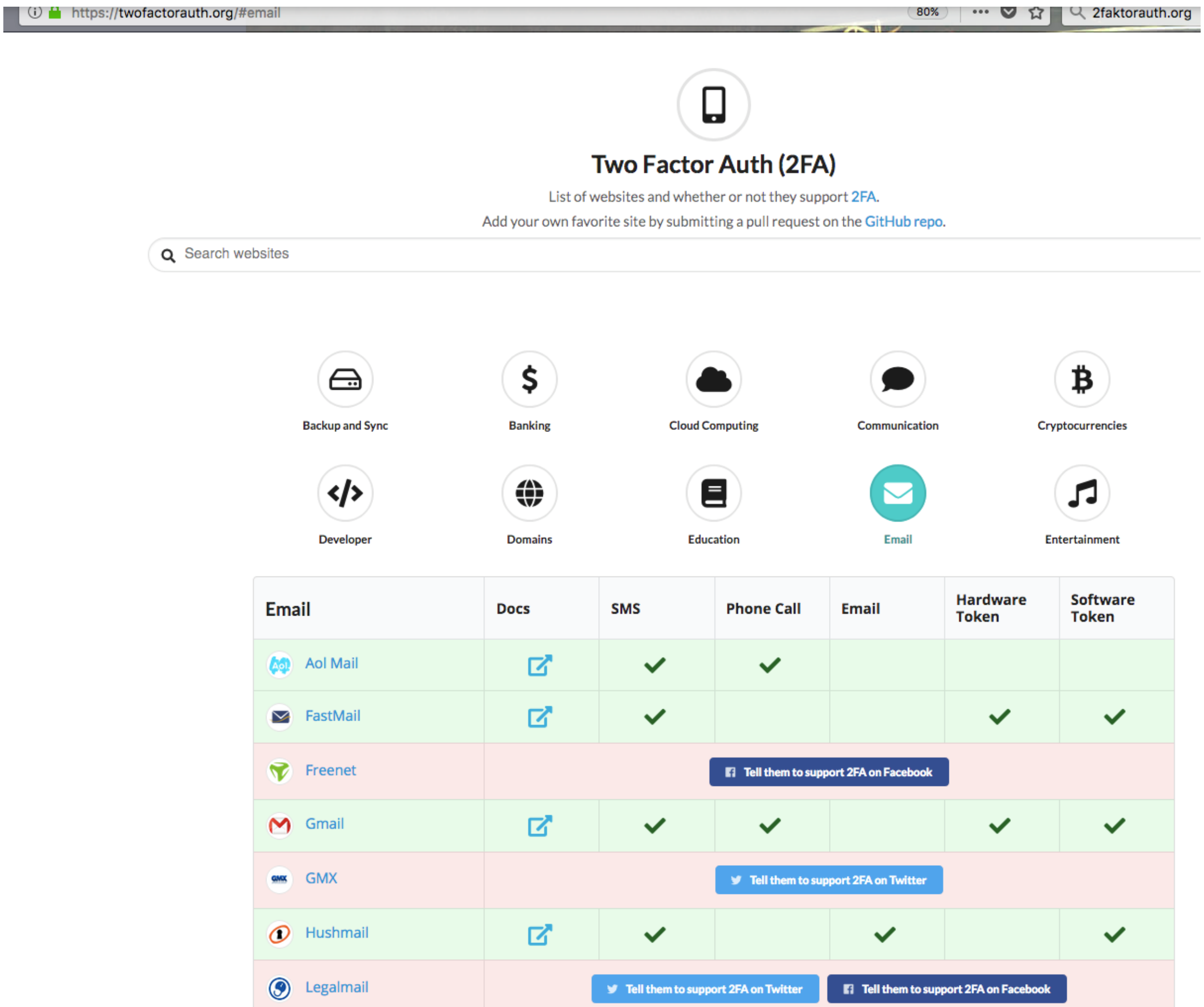
6.3.1.2 Kétfaktoros hitelesítés

A világban rendkívül sok olyan biztonsági incidens történt az elmúlt években – és félő még történni fog a jövőben is – amely során felhasználói adatokat, ezen belül például jelszavakat is elloptak a támadók. Amennyiben kérfaktoros hitelesítés van beállítva a belépésnél, akkor a támadók nem tudnak visszaélni az adatokkal ezen szolgáltatásoknál.

A kétfaktoros hitelesítés egy biztonsági funkció, amely az adott szolgáltatáshoz tartozó jelszóval együtt védi a felhasználói fiókunkat. Ha beállításra kerül a kétfaktoros hitelesítést, a rendszer a bejelentkezési kísérlet megerősítéséhez egy külön bejelentkezési kód megadását kéri minden alkalommal, amikor be szeretnénk lépni a szolgáltatásba. Ezt a kódot több különböző módon megkaphatjuk, például SMS-ben, e-mailben, vagy külön hardveres vagy szoftveres véletlenszám generátor által előállítva. Szerencsére a kétfaktoros hitelesítés egyre elterjedtebb.

A Two Factor Auth (2FA)[6] egy olyan oldal, ahol szolgáltatás típusonként megnézhetjük, hogy melyik szolgáltatás milyen kétfaktoros hitelesítési lehetőségeket biztosít. Ilyen kétfaktoros hitelesítési lehetőségek:

- SMS
- Telefonhívás
- E-mail
- Hardver token (véletlenszám generátor)
- Szoftver token (véletlenszám generátor)



15. ábra Two Factor Auth (2FA) kétfaktorú hitelesítés szolgáltatások

[6] https://twofactorauth.org/

6.3.2 WiFi eszköz biztonsági beállításai

Az otthoni hálózatok kiépítésében is teret nyertek a vezeték nélküli technológiák, mivel kényelmesek, nem kell az egész házat, lakást bekábelezni és egyszerű telepíteni őket. A biztonságukról azonban alapértelmezésben nem gondoskodnak, sőt, a gyári beállítások minden támadó számára ismertek, amivel nem okoz nekik gondot bármelyik nem megfelelően védett otthoni hálózatot ugródeszkaként felhasználni a további támadásaikhoz. Az otthoni vezeték nélküli eszközök alapértelmezésben a saját típusukat adják meg hálózati névnek. Amennyiben ezt nem változtatjuk meg, egy támadó könnyen utánakereshet az eszközünk alapértelmezett beállításainak, megnövelve egy sikeres támadás valószínűségét.

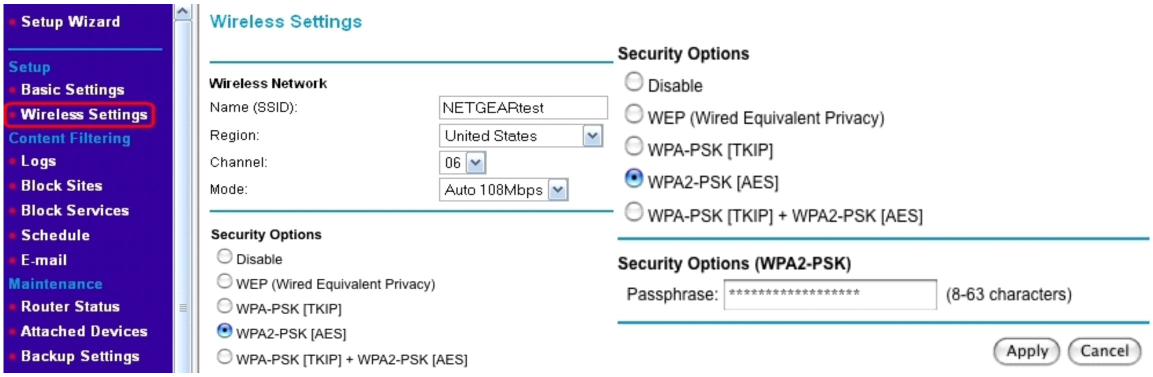
A vezeték nélküli hálózatok hozzáférés-védelmét titkosítással oldják meg, ezt több szinten megtehető. Erre szolgál például a vezetékes kapcsolódással megegyező bizalmasságú hálózat (WEP – Wired Equivalent Privacy – már nem tekinthető biztonságosnak), a WiFi védett hozzáférés (WPA – WiFi Protected Access – ebből is a WPA2 és a WPA3 szabványok, amelyek jelenleg a legfejlettebb biztonságosnak elfogadott módszerek) és ez személyre szabott - módban az előre kiosztott forgalomtitkosító kulcson alapuló védelem (PSK – Pre-Shared Key) – ez utóbbiak alkalmazása erősen javasolt a maximális, 63 karakteres jelszóval együtt.

WPA+3

A Wi-Fi Protected Access (WPA, WPA2 és WPA3) a vezeték nélküli rendszereknek egy, a WEP-nél biztonságosabb protokollja. A létrehozása azért volt indokolt, mert a kutatók több fontos hiányosságot és hibát találtak az előző rendszerben (WEP), illetve a WPA3 javította a WPA2 biztonsági tulajdonságait is. A WPA tartalmazza az IEEE 802.11i szabvány főbb szabályait, és egy átmeneti megoldásnak szánták, amíg a 802.11i szabványt véglegesítik.

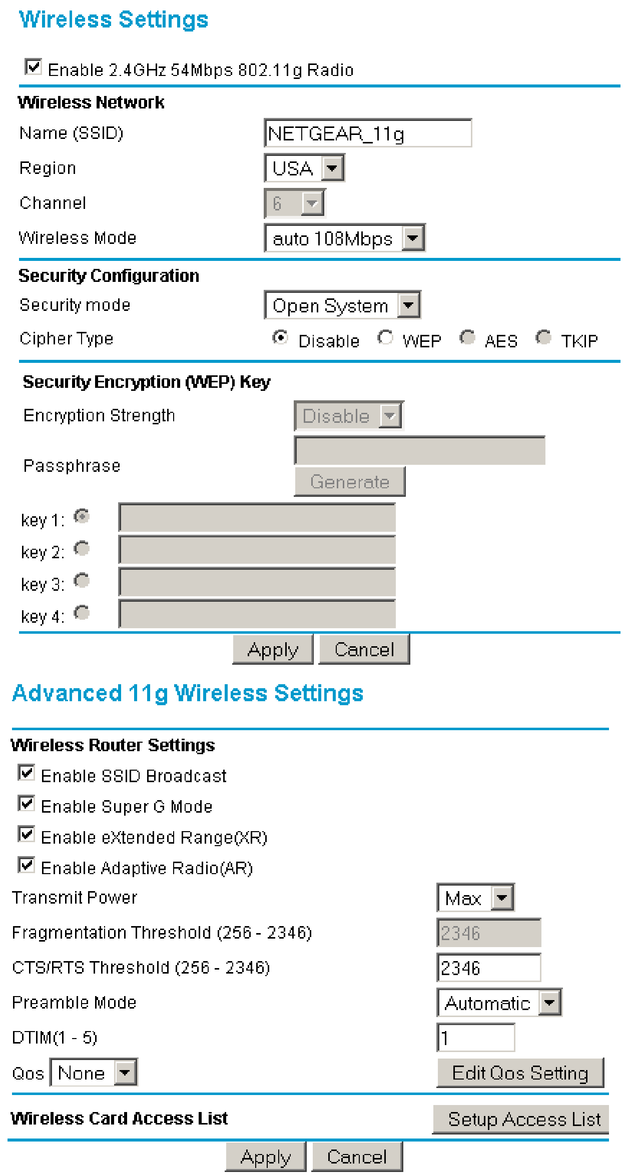
A WPA3 protokoll megnehezíti a bejelentkezési jelszó idegenek általi lehallgatását, mivel a jelszót nem nyílt szövegként, hanem egy jelszó alapú hitelesítési és titkosító kulcs létrehozási protokollt (SAE) alkalmazva juttatja el a háózati eszöznek, ami így nehezebbé teszi a támadó feladatát, mert sokkal tovább kell a forgalmat analizálni egy sikeres támadáshoz. A másik védelmi módszer a hitelesítést követő adatforgalom titkosításához használt ideiglenes titkosító kulcsok kompromittálódása esetében nyújt a kompromittálódott adatforgalom előtti és utáni adatok számára védelmet, mivel ezek titkosításához véletlenszerűen választja meg a kulcsokat, így a teljes forgalom lehallgatásához mindegyik kulcsnak ismertté kellene válnia a támadó számára, mivel egy-egy elcsípett kulccsal nem tud mit kezdeni [t].

A „Personal" (WPA2-PSK) módban, amit a WPA3 funkcionalitással rendelkező hálózati eszközök elterjedésééig valószínűleg a legtöbben választanak otthon és hivatali környezetben, a megadandó jelszónak hosszabbnak kell lennie, mint a jellegzetes 6-8 karakter, amit az átlagfelhasználók általában még elfogadhatónak tartanak.



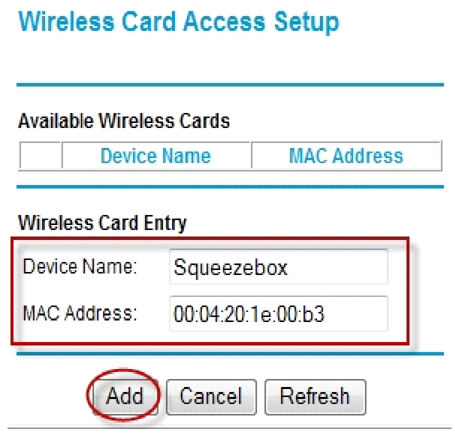
16. ábra Vezetéknélküli hálózat titkosítás beállítás

A védelemért sokat tehetünk az otthoni vezeték nélküli eszköz helyes biztonsági beállításaival és a hozzáférés korlátozásával [ae]. Két alapvető védelmi szint van, egyrészről az eszközbe való bejelentkezési név és jelszó megfelelősége (gyári beállítások felülírása, hálózati név (SSID) megváltoztatás), másrészről a forgalom hozzáférhetetlenné tétele az arra nem jogosultak számára (wifi jelszó).



17. ábra Példa nyílt WiFi rendszer beállításaira

A hálózathoz való hozzáférést korlátozhatjuk a hálózati csatoló egyedi címe szerint is, ennek következtében idegen eszköz nem tud rácsatlakozni a hálózatunkra, másrészről a saját gépünk is csak akkor tud kommunikálni az eszközön keresztül, ha előtte hozzáadtuk a jogosult eszközök listájához.



18. ábra MAC szűrés beállítása WiFi eszközön

Annyiszor ismételhetjük, ahány eszköz címének a befogadására képes a WiFi útválasztónk. Ne felejtsük el az eszközök MAC-címét kitörölni, amennyiben azok kapcsolódása már nem lehetséges. A MAC cím (MAC-address) hat párból álló kombinációja a 0-9 számjegyeknek és az a-f betűknek, tehát ha ilyen látunk, akkor biztosak lehetünk abban, hogy egy hálózatra köthető eszköz második szintű csatolójának a címét tartalmazza ez a furcsa – de a számítógépes hálózatoknál teljesen megszokott – jelsorozat.

Bár nem triviális, de muszáj megemlíteni az eszközök saját szoftverének biztonságát (ideértve az IoT – Internet of Things – Dolgok Internete – internetre csatlakoztatott okoseszközöket [IP kamerák, okosTV-k, okoshűtők, egyéb okoseszközök]), illetve ezek szoftvereinek sérülékenységeit is. Minden célhardver, így a wifi routerek is tartalmaznak egy úgynevezett firmware programot, amely magát az eszközt működteti. Ezek is ember által, gyakran évekkel korábban írt programok, amelyeknek idővel kiderülnek sebezhetőségeik. Rendkívül fontos, hogy az otthoni hálózati eszközeinken is a legfrissebb, ismert biztonsági hibákat nem tartalmazó firmware fusson. A gyártó oldaláról le lehet tölteni a legfrissebb firmware verziót és a router adminisztrációs felületén lehetőség van ennek frissítésére is. Ellenkező esetben áldozatául eshetünk egy támadásnak még akkor is, ha erős titkosításunk van, megváltoztattuk az admin jelszót és úgy gondoljuk, hogy mindent megtettünk a biztonságunk érdekében.

6.3.3 Bluetooth, IrDA

Két, arra alkalmas informatikai eszköz összekapcsolására van még lehetőség Bluetooth és Infravörös (IrDA) kapcsolat kialakításával, illetve fizikai kábellel történő összekapcsolással

is. A Bluetooth és Infravörös kapcsolatok azért érdekesek biztonság szempontjából, mert ezeknek is vannak olyan sérülékenységeik, amelyeken keresztül – például egy állandóan bekapcsolt Bluetooth kapcsolat esetén - a fizikai támadó át tudja venni az eszköz irányítását vagy bele tud ékelődni két Bluetooth-t használó eszköz közötti kommunikációba.

Érdemes a Bluetooth és IrDA kapcsolatokat csak arra az időre aktiválni, amikor használni szeretnénk ezeket. Ezzel nem csak a biztonságunkat erősítjük, de mobil eszköz esetén az akkumlátort is kíméljük.

6.3.4 E-mail

Nagyon gyakori kommunikációs forma az internetes kommunikáció során az egész világon az elektronikus levelezés használata. Az amerikai Radicati piackutató cég 2017-es riportja szerint az üzleti és felhasználói e-mailek száma 2017-ben elérheti a napi 269 milliárdot! Bár manapság kezdik átvenni ez e-mailezés funkcióját az azonnali üzenetküldési szolgáltatások (Facebook Messenger, Viber, Whatsapp, Skype). Az egyszerű e-mail szolgáltatások és programok nyílt szövegként küldik a leveleket a hálózaton keresztül.

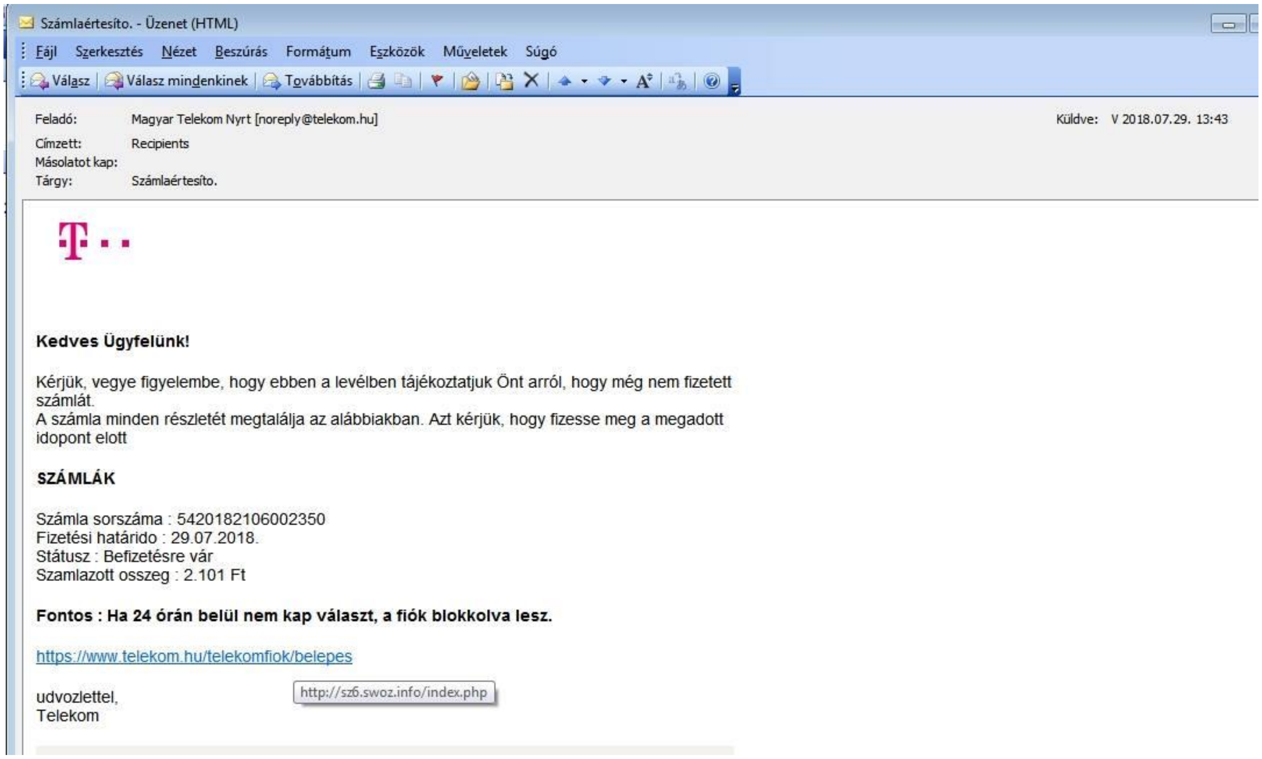
Mivel egy e-mail keresztülhalad számos informatikai rendszeren, míg a címzettjéhez el nem ér, ezeknek a leveleknek a bizalmassági szintje megegyezik egy postai levelezőlapéval. Bárki, aki hozzáfér, olvashatja azt. Ezért azt, hogy csak a címzettek olvashassanak el egy elektronikus levelet, csupán az elektronikus levél titkosítása biztosíthatja. Ide kívánkozik még az e-mail aláírás, mint fogalom. Az e-mail aláírás (nem tévesztendő össze a levelek elektronikus aláírásával) egy olyan előre megírt szöveg, melyet minden egyes kimenő e-mail végére a levelező programunk automatikusan be tud illeszteni. Tipikusan ilyen az elköszönő szöveg, pl. „üdv, Péter”.

E-mail vonatkozásában a legnagyobb kitettséget a csatolmányként küldött rosszindulatú programkódok megnyitása jelenti. Ezek tipikusan vagy neves cégek nevében hamisított levelekben érkeznek, olyan témában, amire a felhasználó ráharap és a kíváncsiság miatt megnyitja a levelet és a csatolmányt. Például fizetési felszólítások, számlák, biztonsági figyelmeztetések, hogy valaki be akart lépni a netbankba, de nagyon gyakori, amikor futárcégek csomagértesítő levelének van álcázva a fertőzést okozó fájl. Ki ne lenne kíváncsi arra, hogy ki és milyen csomagot küldött neki? Ezért kell nagyon óvatosnak lenni ismeretlen feladótól érkező levelekkel, illetve gyanakodni, ha csomag érkezéséről értesítenek, holott nem is vártunk semmit. Nagyon gyakori támadás az, amikor egy word vagy excel dokumentumba makró-vírust rejtenek el, ami a dokumentum megnyitásakor

aktivizálódik. **Makró**nak nevezünk egy olyan rövidítést, amely valamilyen programnyelvi rész, utasítássorozat, vagy felhasználói műveletsorozat helyettesítéseként szerepel. Tekintettel arra, hogy a makrókat a felhasználó is készítheti, semmi akadálya nincsen egy rosszindulatú támadó által készített makró-vírust tartalmazó szöveges dokumentum létrejöttének. Szerencsére a mai vírusvédelmi rendszerek már odafigyelnek a makrókra is.

Egy-egy fájl megnyitását olykor azért kell elkerülni, mert felmerülhet a gyanú, hogy nem azt tartalmazza, amire mi gondolunk – és így jó nyitánya lehet egy sikeres támadásnak, más szóval a csalárd elektronikus levelek általában rosszindulatú programkódot vagy vírust tartalmazhatnak. Egyre gyakoribb, hogy a levél önmaga nem tartalmaz vírust vagy kártékony kódot (ezért a vírusszűrésen sem akad fent) hanem a csatolmányra – vagy a levélben lévő hivatkozásra kattintás után kezd el letöltődni a kártevő. Ha naprakész a vírusvédelmi rendszerünk, akkor jó eséllyel meg tudja akadályozni a kártevő letöltődését.

Az adathalászatoknak is még a mai napig leggyakoribb csatornája az elektronikus levél. Az adathalászat során az eredeti, azonosítást kérő weboldalhoz megszólalásig hasonlító oldalra csalják az áldozatot, ahol az megadja az azonosító adatait és esetleg még egyéb adatokat is, amivel aztán a csalók később megpróbálnak visszaélni. Ide tartozik a banki adatokat bekérő hamisított elektronikus levelek témaköre is. Kaphatunk egy e-mailt és SMS-t is látszólag a bankunktól, amelyik arra kér, hogy látogassunk el az ott megadott linken a bank „speciális" honlapjára és adjuk meg a kért – leggyakrabban érzékeny – információkat. Ezzel kapcsolatosan megjegyzendő, hogy sem a banki, sem egy internetes szolgáltató ügyintézője sosem kérheti el a jelszavunkat telefonon, e-mailben vagy interneten keresztül, azt kizárólag a szolgáltató vagy bank hitelesített weboldalán kell használni. Minden más jellegű kérést, kérdést a jelszavakra (esetleg bankkártya adatokra) vonatkozóan kétkedve és bizalmatlanul javasolt kezelnünk, és az elutasítás után mérlegelhetjük az incidens jelzését is a bank vagy szolgáltató felé. Ez utóbbi azért fontos, mert az ügyfelek tömeges visszajelzései alapján az érintett szervezet egyrészről intézkedést tud tenni az incidens megállítására, másrészről az elkövetők elleni nyomozást is elindíthatja – ami sosem a mi feladatunk, ne is próbálkozzunk vele, mert esetleg a Btk. szerinti tiltott tevékenységekbe futhatunk bele.



19. ábra Adathalász levél példa

Fenti példában azt fontos kiemelnünk, hogy jól látszódik, hogy a kék, aláhúzott levélszövegben lévő hivatkozás és a valós URL – weboldalcím különbözik. Ha rávisszük (De nem kattintunk!) az egerünket az emailekben található hivatkozásokra, akkor pár másodperc múlva megjelenik a tényleges hivatkozás. Ha ez nem egyezik pontosan, vagy nagyon eltérő weboldalnak tűnik, akkor semmiképpen se kattintsunk rá. Fent például árulkodó, hogy a „www.telekom.hu” domain helyett a „sz6.swoz.info” tényleges domain név. Ami nyilvánvalóan nem a szolgáltató oldala.

Kiemelten szeretnénk felhívni a figyelmet a zsarolóvírusokra, mivel ezek a kártevők jellemző módon e-mailben érkeznek meg a felhasználókhoz. Ezért felismerésük az első lépés a megfelelő védekezéshez.

A zsarolóvírusok lefutásához, aktiválódásához felhasználói interakció szükséges. Az e-mailben jellemzően nem maga a vírus érkezik, hanem egy olyan csatolmány, amire a kíváncsi felhasználó rákattint, ezzel elindítva egy olyan programocskát, amely letölti az internetről a tényleges kártevőt, amely ha letöltődött elkezdi áldatlan tevékenységét.

Épp ezért életbevágó, hogy felismerjük az ilyen leveleket. A Symantec cég korábbi statisztikája szerint 89%-ban angolul íródtak az ilyen levelek, a tárgy mezőben pedig az alábbi szavak vannak:

Top malicious email themes

This table shows the most common themes used in email malware subject lines.

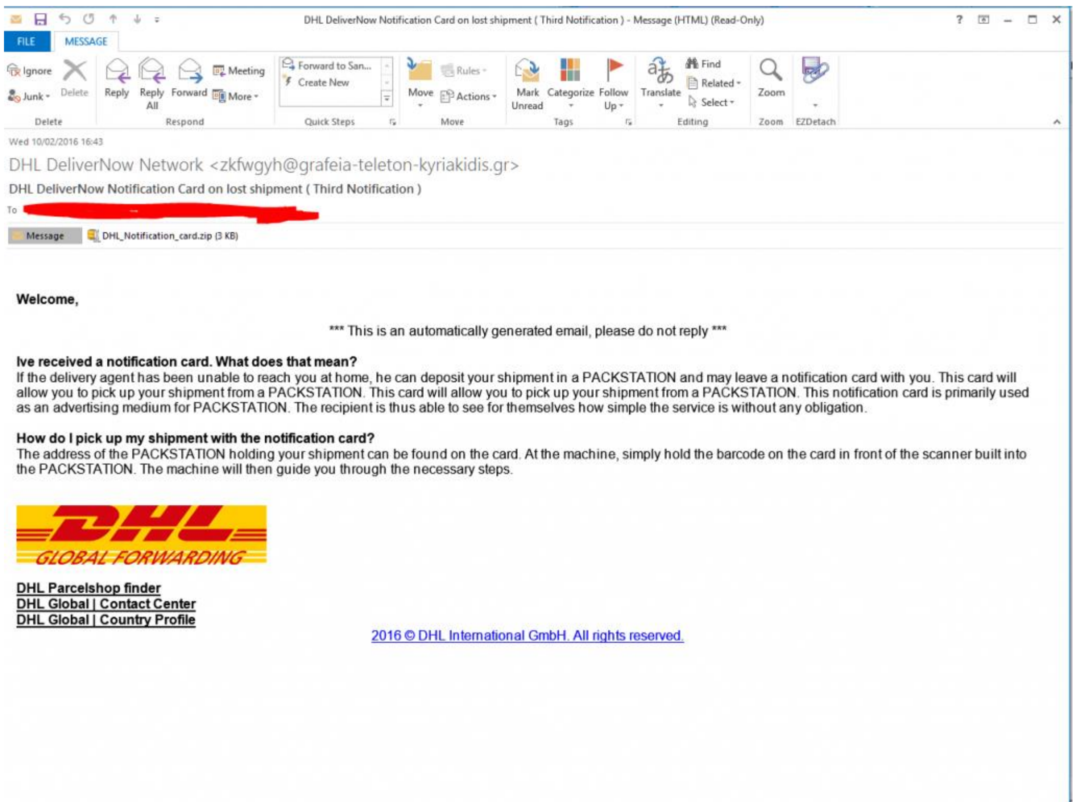
Rank	Subject Topic	Percent
1	Bill	15.9
2	Email Delivery Failure	15.3
3	Legal/Law Enforcement	13.2
4	Scanned Document	11.5
5	Package Delivery	3.9

20. ábra Zsarolóvírust tartalmazó levelek téma szerinti toplistája (2017 Internet Security Threat Report - Symantec) [i]

A kártevőterjesztés egyik fontos feltétele az, hogy a felhasználónak kell jellemzően elindítani a fertőzés első lépését. Nagyon fontos, hogy a támadók szeretnék, ha a felhasználó rákattintana a csatolmányra – vagy a levélben lévő hivatkozásra (linkre), ezért olyan tárgyat és szöveget írnak, ami megüti a felhasználó ingerküszöbét. Például kit ne érdekelne, hogy milyen számlája (bill/invoice) érkezett, ráadásul egy külföldi cégtől? Ezt próbálják kihasználni a támadók, a legtöbb kártevőt terjesztő levél a befizetetlen számlákkal riogatja a felhasználókat. A második legjellemzőbb, hogy egy kézbesíthetetlen levélként érkezik (látszólag) vissza egy levél. Tipikus reakció, hogy ha sikertelenül kézbesített levél érkezik, akkor meg szeretnénk nézni, hogy ez melyik levelünk lehetett, kinek küldük, mit küldtünk a csatolmányban? Ha bedőlünk vagy figyelmetlenek vagyunk és kattintunk, akkor könnyen megvan a baj. Harmadik helyen a különböző jogszabályok megsértése miatti értesítések vannak, ami szintén olyan téma, hogy mindenki kíváncsi, hogy épp miért szeretnék megbüntetni? Negyedik helyen az olyan üres levelek vannak, amelyekhez látszólag egy szkennelt dokumentum van csatolva, mintha egy rosszul konfigurált multifunkcionális gép küldte volna. Mivel nincs információ a szkennelt dokumentumról, a kíváncsi felhasználó könnyen rákattint és már meg is fertőződött. És a ötödik helyen van a csomagküldő szolgáltatók értesítő levelei. Ki ne lenne kíváncsi, hogy milyen csomagja érkezett? A felhasználónak rá kell kattintania a csatolmányra, vagy hivatkozásra, hogy a csomagküldés részleteit megismerje. Nagyon ravasz. A tanulság, hogy ha nem várunk csomagot, akkor ne kattintsunk ilyen levélre. Igaz ez azon nyereményértesítésekre is, ahol több milliós nyereménnyel kecsegtetnek, mert valaki, vagy

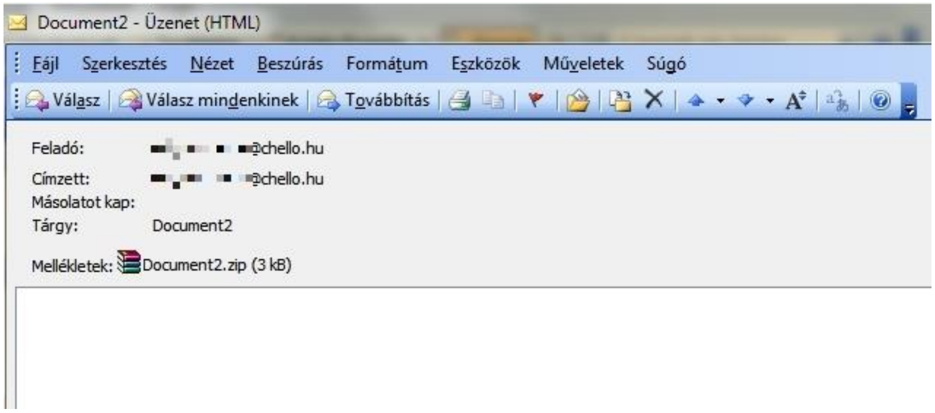
valami kisorsolta a felhasználó e-mail címét. Ilyen nincs. Ha nem játszottunk nem is nyerhetünk! Ha nincs milliomos afrikai bankár nagybácsink, akkor nem is örökölhetünk tőle mesés vagyont.

Lenti példában a DHL nevében egy görög temetkezési vállalat címéről/címét behamisítva küldte a csaló az üzenetét, nyilvánvalóan hamis a levél.



21. ábra Zsarolóvírust tartalmazó e-mail hamisított feladóval

A következő példában a címzett volt feladóként is behamisítva, és semmilyen szöveg vagy magyarázat nem volt a levélben, a felhasználó kíváncsiságára bízva a döntést a csatolmány megnyitásáról.



22. ábra Zsarolóvírust tartalmazó levél, a címzett a behamisított feladó.

6.3.5 Azonnali üzenetküldés

A valós idejű szöveges kommunikáció két vagy több személy között az azonnali üzenetküldés. Sok közösségi program része (Snapchat, Facebook, Skype, Viber, Whatsapp), de külön is használhatók az Instant Messaging (IM), azonnali üzenetküldési szolgáltatások a közösségi alkalmazások során. Megjegyezzük, hogy egyre több IM program része a titkosított üzenetküldés, amelyet, ha nem alapértelmezett, akkor vagy a beállításokban, vagy külön funkcióként érünk el.

Természetesen itt is léteznek sebezhetőségek, amelyek miatt az adataink és gépünk továbbra sincsenek biztonságban. Ezeket a használat során ismerni ajánlott a biztonság megteremtése és fenntartása érdekében. Ilyen veszélyek például a rosszindulatú szoftverek, hátsó kapu hozzáférés, nem kellően korlátozott fájl-hozzáférés. A védelem itt elsősorban bizalmasságot biztosító módszerekkel valósítható meg, mint titkosítás (ami már jellemző a legnépszerűbb üzenetküldőkre), fontos információk titokban tartása, fájl-megosztás korlátozása és természetesen figyelni illik a program integritására, vagyis észlelhetővé kell tenni azt, ha valaki a tudtunk nélkül átírná az azonnali üzenetküldő szoftverét, ami a gépünkön fut (erre szolgál a kódaláírás, amit a digitális aláírásoknál tárgyalunk).

6.3.6 Tűzfalak

A tűzfalak olyan hardveres vagy szoftveres eszközök, melyek egy előre definiált szabályrendszer alapján intézkednek egy hálózat határán a beérkező és kimenő adatelemek engedélyezéséről vagy tiltásáról. Más szóval a tűzfalak az általunk

meghatározott hozzáférési szabályokat kényszerítik ki, tartatják be a kommunikáció során. Tűzfalak tekintetében számos különböző szintű és tudású tűzfal létezik. Felhasználói oldalról a legfontosabb a személyi tűzfal.

Személyi tűzfal (personal firewall): a saját számítógépen működő olyan szoftver, mely az egyes alkalmazások futtatását és hálózati kommunikációikat engedélyezi vagy tiltja, sok esetben öntanuló rendszerben. A személyi tűzfal minden esetben egy futó szoftver a számítógépünkön. A személyi tűzfal vagy az operációs rendszer része, vagy magunk telepíthetjük azt fel a számítógépünkre – például egy biztonsági programcsomag részeként.

A tűzfal feladata, hogy védje a hálózatot a **betörés**ektől, más szóval akadályozza meg a jogosulatlan belépést a hálózatba egy külső helyszínről az előre definiált hozzáférés-védelem kikényszerítésével. A korlátozást szabályok segítségével végzi, mely megmondja a hálózati forgalomról, hogy engedélyezett-e vagy tiltott, emiatt a tűzfal egy szabály-alapú rendszer. Szükség esetén létre lehet hozni további szabályokat a bejövő/kimenő hálózati forgalom kezelésére – erre például egy új játékprogram telepítésekor is szükség lehet, amikor az addig bezárt portokat a játék használatához ki kell nyitnunk, vagyis engedélyeznünk kell.

A tűzfalak jóságát vagy nem megfelelőségét az adja, hogy mennyire képesek kiszűrni a nem kívánt forgalmat **és** mennyire képesek átengedni a várt forgalmat a hálózat minden szintjén. Ehhez képesnek kell lenni szabályokat megfogalmazni számukra, amihez számos segítség, fórum, útmutató található az interneten, de némi kísérletezgetés után saját kútfőből is elsajátítható egy biztonságos környezet megteremtése.

6.4 Adatvédelmi megfontolások, GDPR

Személyes adataink biztonságáról akkor beszélhetünk, ha minden adatunk (legyen a személyiségünkre vagy szokásainkra jellemző) biztonságban van az illetéktelen és jogosulatlan felhasználással, birtoklással szemben, vagyis az **adatvédelem** megvalósul. Sokszor kötelező megadni különböző okokból a személyes adatainkat egyes szervezetek számára, máskor önként adjuk meg az adatainkat, megosztjuk fényképeinket, gondolatainkat a közösségi oldalakon, esetenként arra való tekintet nélkül, hogy ki láthatja, ki kezelheti ezeket és ki nem. Mindez természetesen veszélyeket is rejthet magában. Fontos különbséget tennünk adatvédelem és adat- vagy információbiztonság között. Míg az adatvédelem elsősorban a vonatkozó jogszabályokban használt fogalom, és elsősorban a személyes adatok megfelelő, jogszabály által előírt kezelését értjük alatta,

addig az adat- vagy információbiztonság azon biztonsági kontrollok összességét és elfogadott kockázati szinten való működését jelenti, amelyben az adatok és információk bizalmassága, sértetlensége és rendelkezésre állása biztosított.

A levéltitok védelmét már az 1949. évi XX. törvény is alapelvként rögzítette[7], mely jogszabály 1989-ben módosult és a személyes adatok védelmét tisztán és világosan előírta[8]. Ezt az előírást Magyarország Alaptörvénye is megőrizte[9] és 2011-ben kiegészítette az adatvédelem hatósági ellenőrzésével. Törvényi szinten az első részletes szabályozás 1992-ben jött létre[10], mely már rendelkezett – igaz, elég röviden – az adatbiztonságról (10. §), ezek a szabályok 2011-ben újabb részletekkel gazdagodtak[11], például kártérítési kötelezettség az adatbiztonság megsértésekor, illetve az adatvédelmi audit intézményének bevezetése is ekkor történt. Az EU irányelv által támogatott nemzeti szinten történő adatvédelmet az Európai Unió egységesen kötelezővé tette az adatvédelmi rendelet 2016-os elfogadásával és 2018-as bevezetésével.

6.4.1 GDPR

Az Európai Unió korán felismerte a személyes adatok kezelésének fontosságát, és az uniós egységes szabályrendszer előnyeit ezért 1995-ben létrehozta az Európai Parlament és a Tanács 95/46/EK irányelvét (Európai Adatvédelmi Irányelv) [m] a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról. Ezt követte 2018. május 25-től az Európai Parlament és a Tanács (EU) 2016/679 rendelete (elfogadva 2016. április 27.) „A természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)”. Fenti dokumentumra az angol rövidítéssel GDPR (General Data Protection Regulation) szoktak hivatkozni, még Magyarországon is.

A GDPR kimondja: „A természetes személyek személyes adataik kezelésével összefüggő védelme alapvető jog.” A GDPR ezen felül - részben összhangban a hatályos magyar

[7] 1949. évi XX. törvény 57. § A Magyar Népköztársaság biztosítja a polgárok személyi szabadságát és sérthetetlenségét., a levéltitok és a magánlakás tiszteletbentartását.

[8] 1989. évi XXI. törvény 34. § alapján módosult az 1949 évi XX. törvény: „... 59. § (1) A Magyar Köztársaságban mindenkit megillet a jóhírnévhez, a magánlakás sérthetetlenségéhez, valamint a magántitok és a személyes adatok védelméhez való jog.”

[9] Magyarország Alaptörvénye VI. cikk

(2) Mindenkinek joga van személyes adatai védelméhez, valamint a közérdekû adatok megismeréséhez és terjesztéséhez.

(3) A személyes adatok védelméhez és a közérdekû adatok megismeréséhez való jog érvényesülését sarkalatos törvénnyel létrehozott, független hatóság ellenõrzi.

[10] 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról

[11] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

szabályozással – rendelkezik a személyes adatok kezeléséről, feldolgozásáról, valamint meghatározza az egyes adatkezelésben résztvevők jogait és kötelességeit. Jelen anyagnak nem célja a GDPR részletes kifejtése, annyit azonban mindenkinek érdemes tudnia, létezik ez a rendelet és érdemes utánanéznie, hogy mint magánszemély milyen jogok illetik meg. Ha pedig valamilyen szervezetnek a felelős vezetője a kedves olvasó, akkor azért érdemes utánanéznie, mert az előírások és a büntetési tételek az európai szabályok bevezetésével sokkal szigorúbbá váltak.

Meg kell különböztetni az adatkezelőket az adatfeldolgozóktól. Az adatkezelők olyan személyek, akik vagy a saját maguk által meghatározott célból vagy jogszabály által felhatalmazva kezelik a személyes adatokat[12]. Az adatfeldolgozó feladatát az adatkezelő határozza meg[13], az adatkezelő megbízásából dolgozza fel a szeméyes adatokat, ebből adódóan az ügyfelekkel általában nincs is közvetlen kapcsolatban. Az adatkezelő vagy jogszabályi felhatalmazás, vagy az adattulajdonos felhatalmazása alapján továbbíthatja a személyes adatokat, de harmadik országba csak akkor lehetséges ezt megtenni, ha az adatkezelő garanciákat kap a személyes adatok GDPR által előírt módon történő kezelésére.

Sokszor felmerülő kérdés, hogy kell-e alkalmazni a GDPR rendelkezéseit a közösségi portálokon történő kommunikáció során. A rendelet úgy fogalmaz, hogy ha az adatkezelés semmilyen üzleti célt nem szolgál, akkor nem kell alkalmazni magáncélú csevegésnél az előírásokat, de a közösségi portál üzemeltetőjére – aki az eszközöket biztosítja a közösségi kommunikációhoz – már vonatkoznak ezek a szabályok. A részletes szabályokról javasoljuk tájékozódni a Nemzeti Adatvédelmi és Információszabadság honlapján.[14]

A GDPR létrejöttének célja volt az is, hogy az EU állampolgárainak a személyes adatainak kezelését a cégek és szervezetek komolyabban vegyék. Az adatlopások és egyéb biztonsági incidensek számának növekedése, valamint az évről évre növekvő fenyegetettségek ezt indokolttá teszik. Ezen fenyegetettségek többek között azok, amikor haszonszerzési célból csalással, számítógépes rendszerekhez való hozzáféréssel szereznek – jellemzően pénzügyi – adatokat rólunk, hiszen a feketepiacon a számlaadatoknak értéke van, nem is kicsi. Ennél azonban sokkal értékesebb célpontok lehetnek sok esetben az egészségügyi állapotunkra vonatkozó személyes adatok. Mivel a számlaadatok változnak, egy ellopott bankkártyát le lehet tiltani, egy jelszót meg lehet változtatni, addig az egészségügyi személyes adataink (betegségeink, kórtörténet, állandó gyógyszereink stb.) viszonylag állandónak

[12] GDPR 4. cikk 7.
[13] GDPR 4. cikk 8.
[14] http://naih.hu/felkeszueles-az-adatvedelmi-rendelet-alkalmazasara.html

tekinthetőek, emiatt mind a célzottan támadóknak, mind pedig a célzottabb reklámok küldőinek vagy esetlegesen a zsarolóknak sokkal nagyobb értéket tudnak képviselni.

Az adatok biztonságának kialakítására a GDRP rendelet a 32. cikkében az alábbiakat írja elő az adatkezelő és az adatfeldolgozó számára a tudomány és technológia aktuális állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázatok figyelembe vétele mellett:

- az adatkezelőknek és adatfeldolgozóknak megfelelő technikai és szervezési intézkedéseket kell végrehajtaniuk annak érdekében, hogy a megfelelő szintű adatbiztonságot garantálni tudják, ideértve az alábbiakat is:
    - a személyes adatok álnevesítése és titkosítása
    - a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítása, integritás, rendelkezésre állás és ellenálló képesség
    - fizikai vagy műszaki incidens esetén az arra való képesség, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehessen állítani
    - az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárás kialakítása.

A képzett támadók sokféle módon szerezhetik be a szükséges információkat, például telefonhívásokkal (kikérdezés), adathalászattal (phishing), eltérítéses adathalászattal (pharming), kifigyeléssel (shoulder surfing), vagy személyesen, megtévesztéssel (szélhámosság – social engineering). A szélhámosság módszerei változatosak, nagyon gyakori például az, hogy a szélhámosok valamilyen ürügy révén (pl. üzleti tárgyalás) bejutnak a helyszínre és ott szétnéznek további adatok után kutatva. Ugyanilyen gyakran történik az meg, hogy a szélhámos **információbúvárkodás**t végez, azaz minden fellelhető információt begyűjt későbbi elemzés céljára, akárhol is találja meg azt – nem elfelejtve a szemeteskosarat és a szemeteskukákat sem.

A személyazonosság-lopásnak számos következménye is lehet, lehetnek személyes, pénzügyi, üzleti, jogszabályi következményei is, de mindenképpen kellemetlenséget okozhat. Közvetlen következménye a szélhámosságnak, hogy a személyes adataink és a számítógépes rendszereink mások által hozzáférhetővé váltak, és nagyon valószínű, hogy a begyűjtött adatokat csalásra fogják felhasználni.

A személyazonosság-lopásról jó tudni, hogy leginkább azt jelenti, hogy felveszik más személyazonosságát haszonszerzés céljából. Sűrűn előfordul a kikérdezés, amely során személyes információkat gyűjtenek be megtévesztéssel, vagyis miközben az áldozat például azt hiszi, hogy egy hivatalos közvélemény-kutatóval beszél, a valóságban egy álcázott támadó teszi fel neki a kérdéseket. Fontos, hogy vigyázzunk mások személyes adataira is. Ha elhagyott iratot, bankkártyát találunk, akkor annak képét, fotóját ne osszuk meg a közösségi oldalakon, hanem vigyük be a rendőrségre – ha személyazonosító irat, és a tulaj jelentette, akkor akár körözhetik is. Ha bankkártya, akkor pedig adjuk le az érintett bank valamelyik fiókjában, ahol be tudják a tulajt azonosítani és tudják értesíteni. A bankkártya adatokról bővebben lesz még szó, itt csak annyit jegyeznék meg, hogy az interneten már az alap kártyaadatokkal is lehet sokszor fizetni, így egy közösségi oldalon történő kártyafotó megosztással több kárt tudunk okozni, mint hasznot.

A személyes adatok védelmének legfontosabb oka tehát a személyazonosság-lopás megakadályozása és a csalások megelőzése. Sokat tehetünk ez ellen, ha a böngészés közben néhány egyszerű szabályt betartunk, illetve az igen gyakori kommunikációs felületté előlépett közösségi oldalakon elvégzünk néhány beállítást és figyelembe veszünk néhány szabályt is.

6.4.2 Védelem böngészés közben

Egy webböngészővel egyszerűen meg lehet az egyik internet oldalról egy másikat látogatni, mert a böngésző értelmezni tudja az oldalak közötti váltásra, letöltésre, és megjelenítésre vonatkozó utasításokat. Ezek a HTML (HyperText Markup Language) nyelvben vannak definiálva, amely a WWW (World Wide Web) szabványos nyelvének tekinthető. A HTML formátumú linkek (kereszthivatkozások) segítségével a dokumentumok kapcsolati hálót alkotnak az interneten. A böngészőt eredetileg arra találták ki, hogy szövegeket (lynx), majd képeket (NCSA Mosaic) keressen az interneten és azokat jelenítse is meg – ez a **böngészés** (Az első böngészők után hamarosan megjelentek a keresőmotorok is, de ezek és a böngészőprogramok részletes tárgyalásától el kell, hogy tekintsünk jelen keretek között). Időközben a böngészők már további grafikákat is meg tudtak jeleníteni úgynevezett beépülők (plugin) segítségével, e-maileket lehet velük küldeni, és videokonferenciákat lehet tartani, és még sok más egyébre is használhatók.

Azonban éppen a funkciók sokasága idéz elő komplex konfigurációs lehetőségeket és potenciális biztonsági problémákat. Minél komplikáltabb a böngésző (minél több kiegészítőt tartalmaz), annál több hibalehetőség adódik. Az ilyen programozási hibákat

nevezzük bugnak. A bugok úgy általában minden szoftvert érintenek, mivel nincsenek tökéletes, hibátlanul megírt programok, appok, alkalmazások. A gyártók megpróbálják a bugokat állandóan javítani, és kínálnak javító „foltokat”, más néven javítócsomagokat is (patch), amelyeket fel lehet (és erősen ajánlott is) telepíteni, hogy az adott hibát a felhasználó a saját böngészőjében javíthassa. Ehhez nem kell a böngészőt teljesen letörölni, majd újra visszatelepíteni. Az ilyen „javító programokat” néha patch helyett update-nek, vagy bugfix-nek is nevezik. A fentiek tükrében mindig érdemes használni az automatikus frissítéseket, vagy ha a szoftver erre nem ad lehetőséget, úgy mindig a legfrissebb szoftververziót telepíteni és használni. A szoftverfrissítések telepítésének az a leglényegesebb oka, hogy ezzel lehetőséget kapunk kijavítani egy program hibáját vagy biztonsági kockázatát.

Ezen kívül, mivel a böngészők a weboldalak HTML nyelven megírt kódját értelmezik és jelenítik meg ezért a forráskódba beszúrt olyan parancsokat vagy mini programokat is értelmezik és lefuttatják, amelyekről a felhasználónak nincs is tudomása, mivel magán a weboldal megjelenítésében ez nem okoz változást. Ha egy hacker feltör egy weboldalt és ki akarja használni a weboldal népszerűségét arra, hogy gyanútlan felhasználókat fertőzzön meg, akkor az oldal forráskódjába beszúr egy olyan kis mini programot (scriptet), ami a weboldalon nem látszódik, de a böngésző értelmezi és egy másik oldalról elkezd vírust telepíteni a felhasználó gépére. Ha a támadónak sikerül egy hirdetéssel vagy egyéb aktivitással nagyobb számú látogatót az oldalra csalni – akik emiatt nagyobb arányban fognak megfertőződni, akkor ezt a támadást watering hole néven szokták emlegetni (a sivatagban az itatóhoz, víznyerő helyhez nagy tömegben érkező vadállatokra és az itt rájuk támadó ragadozókra utaló hasonlóság miatt). Ez a támadás addig folyhat, amíg valaki nem szól az oldal gazdájának, vagy a böngészők fekete listára nem teszik az oldalt és jelzik a felhasználónak, hogy az oldal rosszindulatú programot terjeszt. Az ilyen fertőzés ellen a legjobb módszer a naprakész vírusirtó program, amely már letöltés előtt, vagy közben megfogja a kártevőt és figyelmezteti a felhasználót. Sajnos ilyen fertőzési próbálkozással bármilyen weboldalon összefuthatunk egy papírbolt weboldalától az iskolai weboldalakon át egy magánszemély privát oldaláig bezárólag. Nem kell, hogy illegális vagy felnőtt tartalmakat megosztó oldalakra látogassunk.

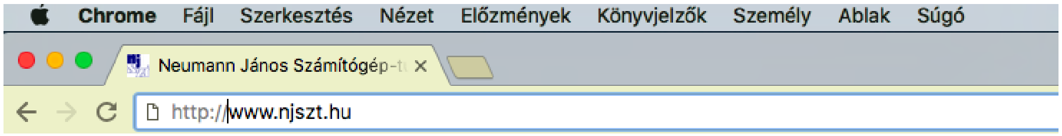
Az internet-használat biztonsága alapvető fontosságú digitális értékeink védelméhez. Nagyon fontos tudatában lenni annak, hogy bizonyos online tevékenységeket (vásárlás, pénzügyi tranzakciók, internetes bankolás, internetes számlafizetés) csak biztonságos web-oldalakon szabad végrehajtani. Meg kell tanulni azt, hogy hogyan ismerhetjük fel a biztonságos weboldalakat jelölő elemeket, mint például a https előtag és a zár-szimbólum.

Az internetes vásárláskor, tranzakciók generálásakor számos esetben űrlapokat kell kitöltenünk, ahol lehetőség van a megfelelő engedélyezési, tiltási, automatikus kitöltési, automatikus mentési beállítások kiválasztására.

A magánélet védelme érdekében fontos – főleg nyilvános helyeken (pl. internet-kávézó, nyílt hozzáférési pontok), hogy megtanuljuk, hogyan kell személyes adatainkat törölni a böngészőből, különös tekintettel a böngészési előzményekre, könyvjelzőkre, ideiglenesen tárolt internet fájlokra, az elmentett jelszavakra, sütikre, automatikusan kitöltött űrlap-adatokra. Ez akkor is fontos, amikor ilyen helyeken a webalapú levelező fiókunkat használjuk.

6.4.3 A látogatott oldalak biztonsága

A WWW tulajdonképpen elkülönített dokumentumokat fog össze hálózatban. Linkek (kereszthivatkozások) segítségével fogalomról fogalomra, dokumentumról dokumentumra, weboldalról weboldalra lehet ugrani. A WWW világszerte felkínálja a legkülönbözőbb jellegű információkat, szövegeket, képeket, grafikákat, hangokat, videókat, az emberiség csaknem összes digitalizált tudása elérhető a weboldalakon keresztül. És ez - nap mint nap - több százezer oldallal, egyes kutatások szerint 600.000-800.000 új oldallal is bővül, ugyanakkor csökkenő tendenciát mutat. A nyomtatott sajtó (kiadók), nyomtatott publikációk, egyetemek, magánszemélyek, múzeumok, nemzeti és nemzetközi szervezetek, egyesületek, vállalatok stb. kínálnak számtalan információt.



23. ábra Uniform Resource Locator - URL

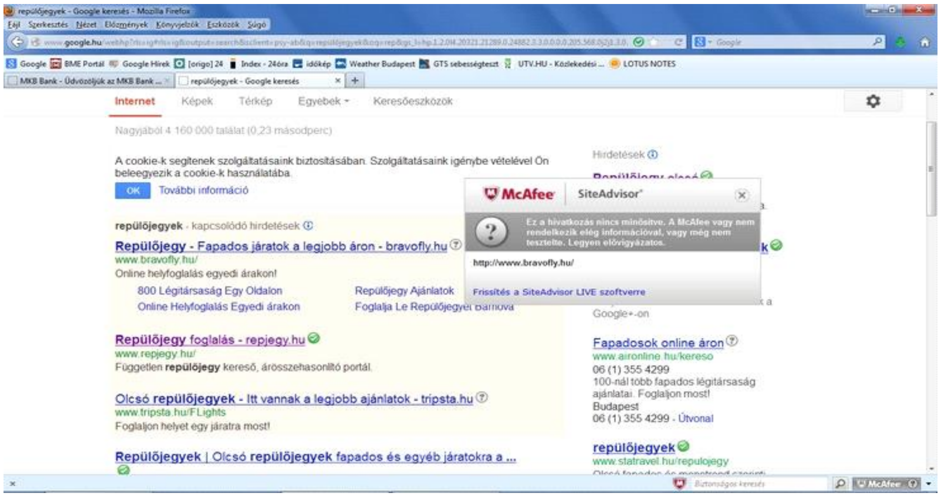
Minden weboldalnak van egy neve, az úgynevezett URL (Uniform Resource Locator), amit böngészővel lehet elérni, azaz a böngésző címsávjába kell beírni. A névhez egy IP-címnek is kell tartoznia, ami alapján a hálózati kapcsolat létrejöhet. Az URL áll egy protokoll-megnevezésből (http://), egy domain névből (www.njszt.hu) és egy oldalnévből (index.html), amely azonban nem minden esetben jelenik meg.

A nevek és címek összerendelését segíti a **DNS**, Domain Name System, magyarul a domain név rendszer [l]. A DNS rendszer a domaineket (tartományokat) kezelő, a világon több ezer szerverre elosztott hierarchikus adatbázis-rendszer. Ezek a domainek vagy tartományok

úgynevezett zónákra vannak elosztva, ezekért egymástól független adminisztrátorok felelősek. A nevek rendezése a múltban nagyon szigorúan kötődött a **DNS-végződés**hez, így például egy „valami.university.edu” névből azonnal lehetett tudni, hogy ez a szerver az Amerikai Egyesült Államokban van és egy oktatási intézmény áll mögötte. Hasonlóan a fenti példa „.hu” végződése egyértelműsítette, hogy egy magyarországi (HUngary) domaint takarhat csupán. Az egyes tartományokat (pl. .hu) felosztották zónákra (pl. ecdl.hu), ahol minden egyes IP-címet a zóna-felelős menedzsel és rendel hozzá. A zónába a tartományon keresztül vezet az út, tehát a rendszer lelke a legfelső szintű tartomány-vezérlő szerverek összessége. Aki ide nincs bejegyezve – közvetlenül vagy egy zónán keresztül, azt nem lehetséges névvel megtalálni (pl. www.ecdl.hu), csak közvetlenül az IP-címén szólítható meg (193.225.14.73). Ez nyilván sokkal kényelmetlenebb megoldás.

A World Wide Web-en a Hypertext Markup Language (HTML) dokumentumnyelvet használják. Ennek alkalmazásával lehet kereszthivatkozásokat (linkeket) készíteni más dokumentumokhoz, valamint tetszés szerinti nagyszámú képet, filmet, vagy hangot mellékelni. A HTML-adatokat többnyire a HTTP (Hypertext Transfer Protocol) kommunikációs protokoll segítségével közvetítik.

A támadók jellemzően az internet kevésbé ellenőrzött részein bújnak meg, **ál weboldal**akat készítenek (melyek megszólalásig hasonlítanak az eredetire, de mögöttük már a támadó áll), illegális tartalmakat árulnak, vagy rosszindulatú programokat, szkripteket (parancssori programok), linkeket szeretnének letölteni/letöltetni a felhasználó gépére, és egyébként is, szeretnének a mások számítógépei és adatai felett tulajdonosi jogköröket gyakorolni jogosulatlanul. A káros tartalmaknak azonban vannak olyan jellemzőik, amiket a védelmi programok képesek többé-kevésbé beazonosítani, és a felhasználót erre figyelmeztetni. Az egyik ilyen védelmi szolgáltatás a „SiteAdvisor”, ami a weboldalakat minősíti és a minősítés alapján tanácsokkal látja el a felhasználót az oldallal kapcsolatosan.



24. ábra McAfee SiteAdvisor – a megbízható weboldalakért

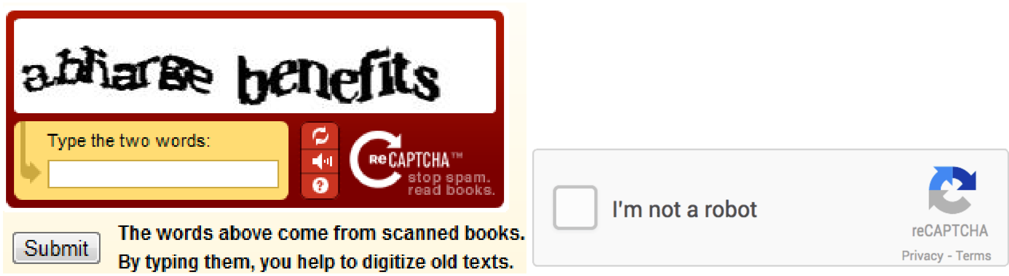
Például egy online pénzügyi tranzakció elvégzésekor, vagy személyes adataink megadásakor, azonosító és jelszó megadásakor a weboldal biztonságának biztosításához ragaszkodni kell. Ennek leggyakoribb eszköze a biztonságos böngészés, a https (secure http) protokoll használata. Ma már a keresőoldalak is https csatornán keresztül érhetőek el, ugyanakkor számos keresési eredmény – weboldal még mindig http – nem titkosított csatornán tekinthető meg. Ezzel szemben szinte minden online bank, online webáruház ma már csak a biztonságos weboldalt jelző https előtaggal érhető el. A biztonságos webhasználatot számos más funkció is támogatja. Például nagy segítség a felhasználónak, ha a böngésző automatikusan ellenőrzi a weboldal tanúsítványának megbízhatóságát és az ellenőrzés eredményét színkóddal jelzi (zöld pipa jelzi azt, ha a böngésző mindent rendben talált, sárga szín jelzi, ha nincs minden rendben, és piros szín esetében pedig erősen javasolt a weboldal meglátogatásától tartózkodni). A biztonságot erősíti az is, ha az internetbank pár perc üresjárat után megszakítja a kapcsolódást (időtúllépés), ez megnehezíti egy esetleges lehallgató dolgát is.



25. ábra Biztonságos weboldal jele, a lakat ikon

A **biztonságos weboldal** jele a lakat-ikon (a színe, megjelenítése, böngészőnként változik), egy lezárt lakat jelzi azt (a https-en kívül), hogy itt most titkosított forgalomról van szó a webszerver és a felhasználó számítógépén futó böngésző között.

Szintén az automatizált támadások elleni védelemre szolgál a „**captcha**” [m]. Ez a mozaikszó a „**C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part” hosszú kifejezésből ered, ami gyakorlatilag annyit tesz, hogy hogyan tudja megkülönböztetni egy számítógép a hozzá forduló embert egy másik (esetleg támadó szándékú) programtól („Nem vagyok robot.”). Leggyakrabban egy olyan módon eltorzított szöveg felismerését jelenti, mely meghaladja egy számítógépes program képességeit, de nem okoz gondot az embernek.



26. ábra Captchák

Ezen kívül léteznek más típusú captcha-k, például amelyeken képeket kell megjelölni bizonyos szempont szerint. Például ”Válaszd ki azokat a képeket, amelyeken közlekedési táblák/autók/épületek/stb. vannak”.

6.4.4 Aktív tartalmak és a biztonság

A legtöbb böngésző alapbeállításként lehetővé teszi olyan funkciók végrehajtását, amelyek a látogatott oldalakon elrejtve vannak jelen, vagy interaktív, esetleg animált tartalmat jelenítenek meg. Az ilyen rejtett programrészeket „szkripteknek”, az interaktív/animált tartalmakat pedig „aktív tartalmaknak” nevezzük. A legismertebbek a sütik (cookie), Javaappletek, ActiveX Control-ok, JavaScript, VBScript és a Flash.

- Sütik: A sütik (cookie) a korábbi felhasználói történések, a böngészési állapotok megőrzését és reprodukálhatóságát biztosítják a webes böngészés során. A sütik által rögzíteni kívánt információkat a webszerver határozza meg. A sütiket mind a webszerver, mind a böngésző eltárolja. Ennek eredményeként egy későbbi

bejelentkezést követően a felhasználó ott tudja folytatni például a webáruházi kosarának feltöltését, ahol abbahagyta. A sütik megkönnyítik a böngészést, de felvetnek néhány biztonsági problémát is (15). Egyrészről a sütik révén a webszerver gazdája rögzítheti tevékenységeinket az adott webszerveren. A sütik tetszőleges adatokat képesek elraktározni, ideértve a látogatott weboldalak címeit, azokat a kulcsszavakat, amelyekre kereséseket indítottunk és képesek eltárolni a különböző weboldalakon történő bejelentkezéseink adatait is a jelszavainkkal együtt. Ebből következik, hogy ha egy támadó hozzáfér a gépünkhöz és ki tudja olvasni a böngészőnk által eltárolt sütikből az adott weboldalhoz tartozó jelszavainkat – amennyiben azokat nem, vagy gyengén titkosítva tartalmazza a süti, akkor azokat máris fel tudja használni.

- Java appletek: A Java egy univerzális programozási nyelv, amit a Sun Microsystems eredetileg házi készülékek irányítására fejlesztett ki, azonban nagyon hamar elterjedt programozási nyelvvé vált az alkalmazások minden területén. Minthogy független a hardvertől és az operációs rendszertől, nagy népszerűségnek örvendett a Java, és a fejlesztők mindig hozzáigazították a mindenkori új igényekhez. Ma már az Oracle fejleszti tovább. A Java programok azon különleges fajtáját Java appleteknek nevezzük, melyeket a weboldalakba be lehet illeszteni, ami a weboldal meglátogatásakor letöltődik a felhasználó gépére. Java alapú megvalósítást használhatnak például a képgalériák, online játékok, stb.
- ActiveX: A Microsoft az ActiveX-et a Java konkurenciájaként fejlesztette ki, ebben a funkciókat szorosan a Windows operációs rendszerekhez igazították, így más operációs rendszerek ezeket a lehetőségeket nem is tudják használni. Az olyan ActiveX elemeket, amelyek aktív tartalmakként beilleszthetők a weboldalakba, ActiveX vezérlőknek (ActiveX Control) nevezzük. Fontos tudni, hogy az ActiveX program a bejelentkezett felhasználó gépén teljes jogosultsággal működik, minden korlátozás nélkül.
- Javascript: A JavaScriptet a Netscape fejlesztette ki aktív tartalomként való alkalmazásra a weboldalakon. A JavaScript a Jáván alapuló script nyelv, olyan programozási nyelv, amely a felhasználónál szövegformában van jelen, és külön e célra alkalmazott értelmezőprogram (interpretáló) által lehet alkalmazni. Alkalmazható például űrlapok kitöltésének ellenőrzésére, látogatottság számlálásra vagy képek cseréjére (ha ráviszem az egér mutatóját egy képre, akkor egy másik

[15] https://www.bitdefender.com/support/cookie-threats-1.html

jelenik meg). Fontos veszélye, hogy lehetővé teszi ActiveX Control-ok aktivizálását, amelyeket már egyszer a számítógépre telepítettünk, és ezáltal ugyanolyan jogokkal bírnak, mint a helyi telepítésű program.

- VBScript: A VBScript ugyancsak a Microsoft által kifejlesztett programozási nyelv, amely a Visual Basic programozási nyelvre támaszkodik és szorosan kapcsolódik a Windows operációs rendszerekhez. VBScripttel is ki lehet egészíteni a weboldalakat aktív elemekkel. Mindenesetre az Internet Explorer az egyetlen böngésző, amely kiegészítők nélkül képes a VBScriptet a weboldalakon működtetni. Szintén képes ActiveX vezérlésére.
- Flash: 1996-ban vezette be a Macromedia (jelenleg az Adobe) a flash-technológiát, ami nagyon gyorsan teret hódított. Egy időben rendkívül sok weboldalon volt flash alapú tartalom, mára azonban ez a technológia egyre kevésbé népszerű, elterjedtsége jelentősen csökkent. A Flash alapvetően egy grafikai szerkesztő, amely animációt és interaktivitást is lehetővé tesz. Ezzel együtt a felhasználók gépein a flash lejátszását lehetővé tévő Flash Player továbbra is igen elterjedt, így a támadók a lejátszóprogramok biztonsági réseit is kihasználják, hogy az áldozat gépére valamilyen káros programot telepítsenek vagy az áldozat gépéről információkat szerezzenek.

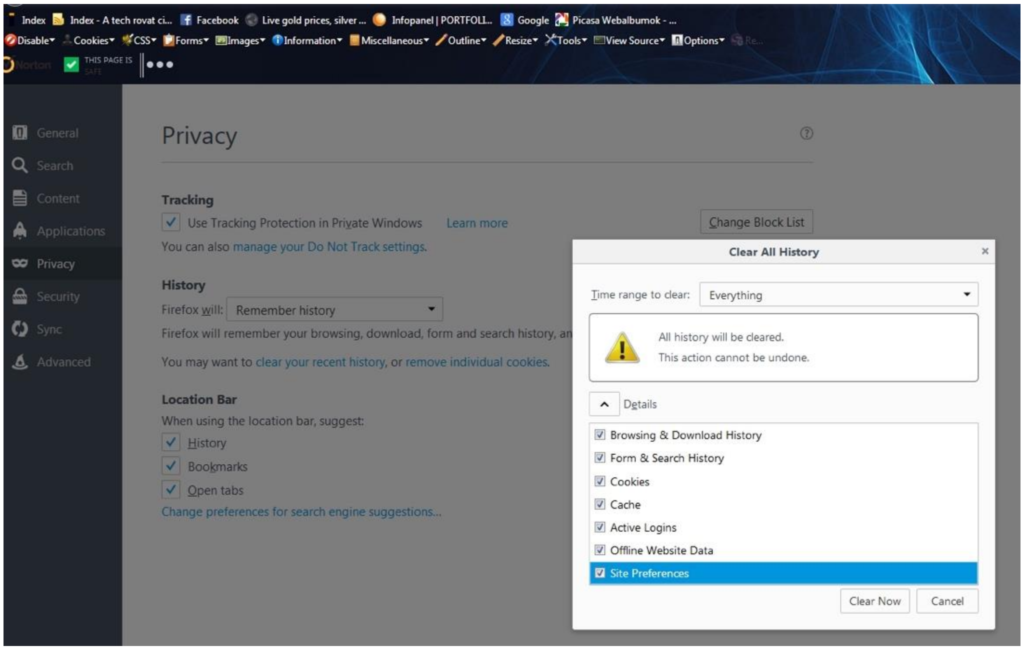
Fordítsunk kiemelt figyelmet az aktív tartalmakat megjelenítő programjaink frissítésére (Automatikus frissítés beállítása számítógépeinken és okoseszközeinken is!), mivel időről időre ismertté válnak sérülékenységek, amelyek ezekre a programokra vonatkoznak. Mivel ezek a programok gyakorlatilag milliónyi felhasználó gépén futnak, potenciális célpontjai az internetes támadásoknak, vírusoknak. Ha sérülékeny verziót használunk – például egy régi Adobe Flash Playert, akkor ennek sérülékenységeit kihasználva egy támadó kémprogramot vagy egyéb kártékony kódot telepíthet a számítógépre. Telepítéseken kívül egyszeri beavatkozásokat is végre lehet hajtani aktív tartalmakkal egy weboldal látogatása során, melyek kétségkívül károsan hathatnak a felhasználó adataira. Hálózatbiztonsági szempontból ezért csak azt tudjuk tanácsolni, hogy az aktív tartalmakat elvből kapcsoljuk ki, vagy korlátozzuk (például Firefox böngészőben a „NoScript plugin”). Ennek hatására a felhasználó veszíteni fog valamit a kényelemből, tudniillik sok weboldal úgy van elkészítve, hogy csak akkor lehet őket rendesen megjeleníteni, ha az aktív tartalmak engedélyezve vannak, ellenben a biztonsági szintet növelte ezáltal.

6.4.5 A böngészőben tárolt adatok biztonsága

Böngészés során – akár tudunk róla, akár nem – számos adat és szokás naplózódik a meglátogatott oldalak kapcsán.

- előzmények: a meglátogatott oldalak listája időrendi sorrendben.
- űrlapadatok: a böngészés során kitöltött űrlapok elmentett adatai (ideértve egy bejelentkezési ablak felhasználói név megadásának dobozkáját is), különösen akkor, ha az automatikus kiegészítés funkciót engedélyeztük.
- sütik: a látogatott oldalakkal kapcsolatos olyan személyes információk, melyek a webszerveren és a saját gépünkön is eltárolódnak a böngészési adatok dinamikus kezelése, későbbi felhasználhatósága érdekében.
- jelszavak: a bejelentkezések megismétlését megkönnyíti, ha a jelszó beírását követően elfogadjuk a böngésző azon javaslatát, hogy elmenti az éppen most beírt jelszót – de ez egyben kockázatot is képez, ha ennek tárolása nem megfelelően történik.

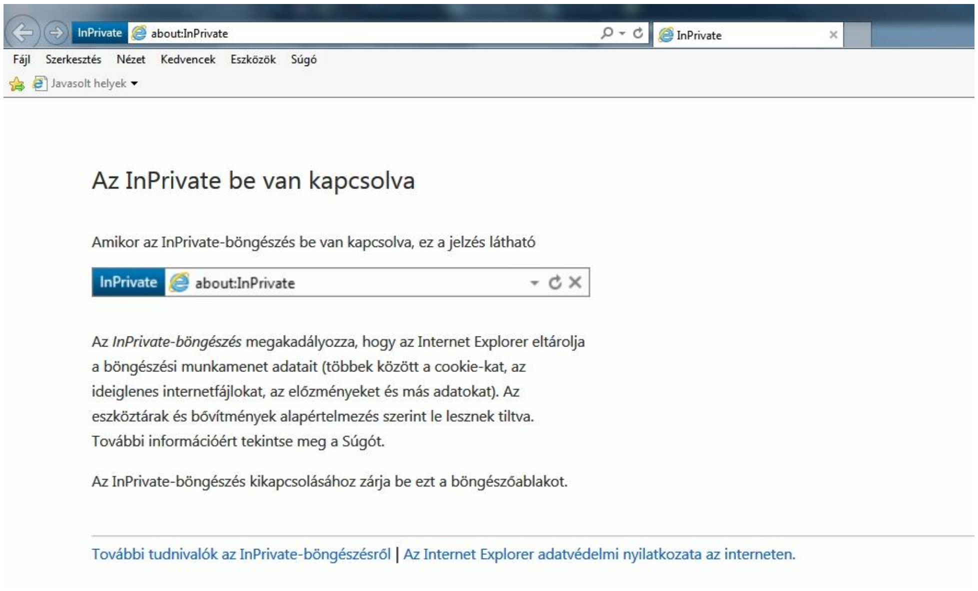
Az **automatikus kiegészítés** funkció használatával az űrlapok kitöltése egyszerűbbé és gyorsabbá válik, hiszen nem kell minden egyes esetben begépelnünk a teljes szöveget, mert a böngésző az előzetesen eltárolt adatokból az első pár karakter leütése után automatikusan felkínálja az oda illeszkedőket, legyen az bejelentkezési név, bankszámlaszám vagy e-mail cím. Az automatikus kiegészítés használata tehát jelentősen felgyorsíthatja egy-egy ismétlődő adatbevitelt is tartalmazó online űrlap kitöltését. De fontos arra is odafigyelni, hogy a böngésző által ez az adat törölhető is egyben, hiszen a tárolása veszélyeket is rejt magában. Ezeket az adatokat időnként javasolt a magánszféra védelme érdekében törölni, különösen akkor, ha nem a saját számítógépünkön internetezünk, hanem például egy internet-kávézóban levő gépen, közösen használt felhasználói név alatt.



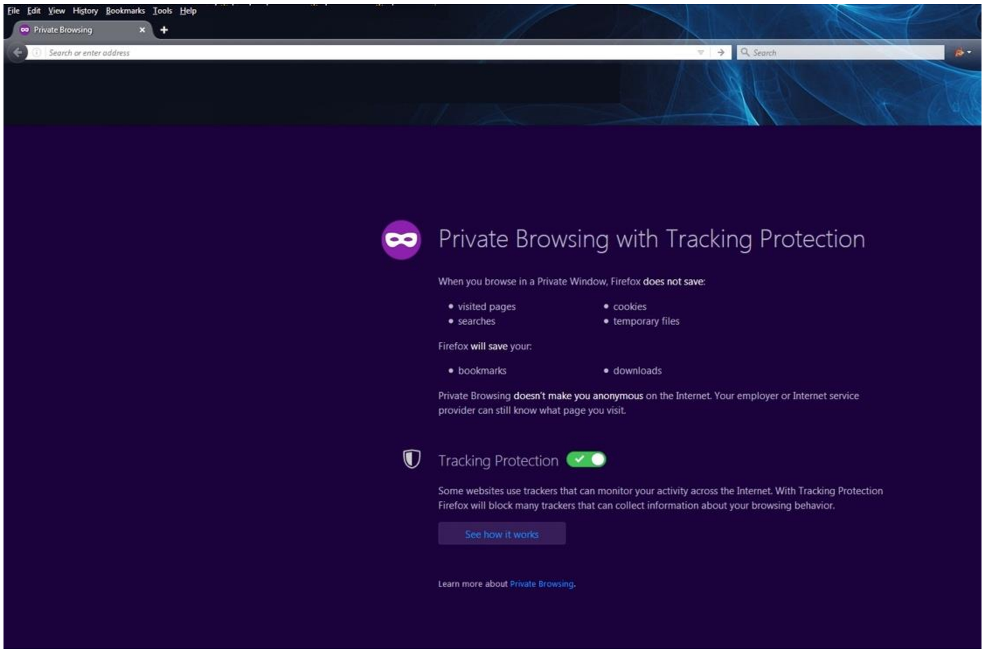
27. ábra Böngészési adatok törlése Firefoxban

A böngészőben eltárolt személyes adatok törlését időről-időre javasolt elvégezni - amennyiben a tárolt jelszavak mindegyikére emlékezünk vagy más helyen (pl. jelszógenerátor programban) is megvannak. Különösen fontos a böngészési adatok törlése nyilvános internetes állomásokon vagy több személy által használt közös felhasználói fiókok esetében, de az otthoni gépünkön sem árthat.

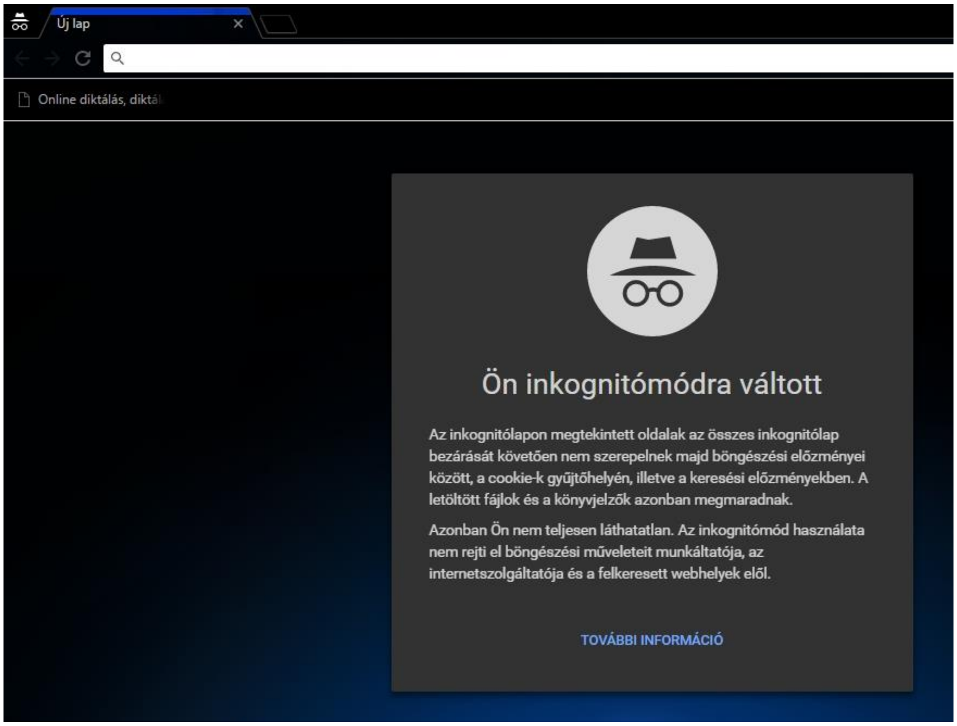
Az összes népszerű böngészőben megtalálható már olyan üzemmódú böngésző ablak, amelyet használva, a böngészett weboldalak adatai (sütik, url-ek, látogatott oldalak, kitöltött form-ok adatai, jelszavak stb.) nem tárolódnak el. Ezeket böngészőnként máshogy hívják. Az alábbi képeken az Internet Explorer (InPrivate böngészés), a Firefox (Private browsing) és a Chrome (Inkognitó mód) biztonságos böngészési ablakait láthatjuk.



28. ábra Inprivate böngésző üzemmód Internet Explorer



29. ábra Privát böngészés Firefox böngészőben



30. ábra Inkognító üzemmód Chrome böngészőben

6.4.6 Bizalmassági eszközök közösségi oldalakon

A közösségi oldalak terjedésével nagyon sok információ, személyes adat kikerülhet a nyilvános – bárki által elérhető – hálózatra, a nem megfelelő beállítások vagy az automatikus alapértelmezett beállítások következtében. Fontos megérteni, hogy bizalmas információkat közösségi oldalon miért nem szabad közzétenni, és hogyan kell azoknak a védelmi beállításait megvalósítani, valamint folyamatosan kontrollálni.

A közösségi oldalakon történő kontrollált és végiggondolt megjelenés azért is fontos, hogy a lehetséges veszélyeket képesek legyünk elkerülni, úgymint internetes zaklatás (cyber bullying), szexuális kizsákmányolás (grooming), félrevezető/veszélyes információk, hamis személyazonosságok, csalárd linkek vagy üzenetek használatából, elfogadásából adódó károk.

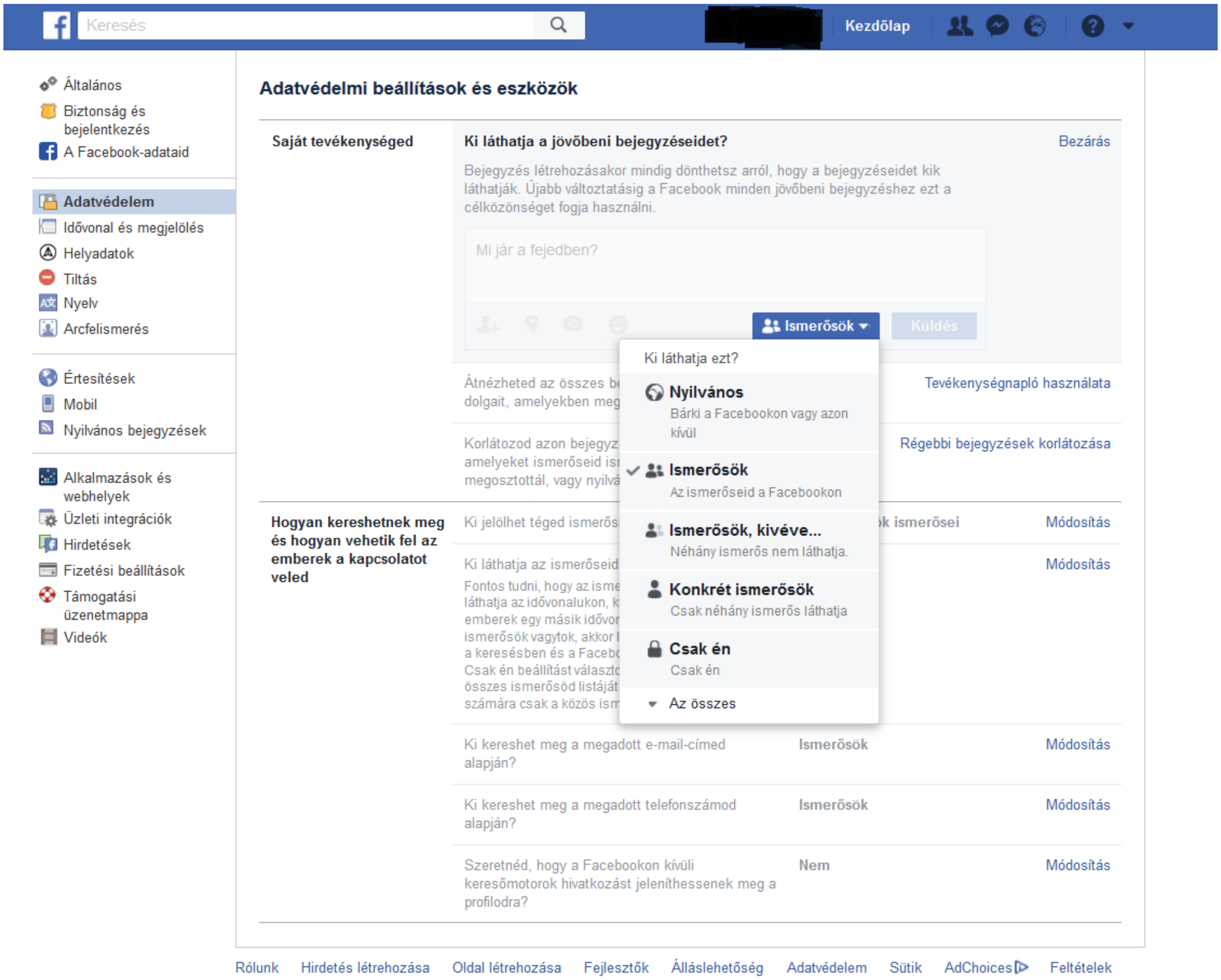
Nagyon könnyen a bizalmunkba férkőzhetnek a támadók akkor, ha olyan bensőséges adatokat adunk meg a közösségi hálózatokon, mint például a becenevünk, de fizikai közelségbe is kerülhetünk velük, ha a nyaralási dátumunkat a lakcímünkkel együtt hozzuk nyilvánosságra. Tekintettel arra, hogy a virtuális támadók potenciális száma jóval nagyobb, mint a valós térben várható támadók száma, a kockázat ennek megfelelően számítható.

Ilyen veszélyt kevésbé rejt a zenei érdeklődés és a kedvenc televízió műsor megadása, mivel ezek egyrészről több helyről hozzáférhető adatok, másrészről többek által megismerhető adatok, mint a becenév. Egy szexuális bűnöző számára megkönnyítheti a szexuális kizsákmányolás előkészítését minden apró információ, amit megadunk a közösségi oldalakon, ez egy ismert és nagyon veszélyes fenyegetés itt.

Az eredménye annak, ha egy közösségi oldalon a személyes adatokat a nyilvánosság számára hozzáférhetővé tennénk az, hogy a személyes adatokat bárki megnézheti, a keresőprogramok beindexelik és akár vadidegenek számára is megjelenítik, mint keresési találatok. A közösségi média használatakor nemcsak azok olvashatják adatainkat, akik barátságosan viseltetnek irányunkban, hanem azok is, akiknek esetleg valamelyik megnyilvánulásunk nem tetszik, és ezt **internetes zaklatás**ban fejezik ki.

Ezt elkerülni – illetve a kockázatait csökkenteni – három módszerrel lehet:

- barátaink megválasztásánál óvatosan járunk el vagy a kellemetlen barátot töröljük, és
- az adatvédelmi beállításokat olyan szigorúan szabjuk meg, amennyire csak tudjuk, hogy a barátainkon kívül más lehetőleg ne olvashassa bejegyzéseinket és ne nézegethesse a feltöltött képeinket, továbbá
- figyeljünk arra, hogy ki léphet velünk kapcsolatba – ha nem szükséges, a közvetlen kapcsolat-felvételt ne engedélyezzük senki ismeretlennek, csak annak, akit már valaki az ismerősi körünkben – valamilyen módon – hitelesített saját ismerőseként.



31. ábra Adatvédelmi beállítások közösségi oldalon

Az előző ábrán az adatvédelmi beállításokat és azok közül a láthatóság beállítására vonatkozó lehetőségeket mutattuk be. A közösségi oldalak számos beállítási lehetőséget kínálnak a felhasználók számára, amelyekkel javasolt élni. Az alábbi témakörök köré csoportosulnak a beállítások – például – az egyik legkedveltebb közösségi oldalon, a Facebookon:

- Ki láthatja a dolgaimat?
- Ki láthatja az ismerőseim listáját?
- Ki léphet velem kapcsolatba?
- Ki találhat rám?

A Facebookon ezen kívül számos egyéb módon is növelhetjük a biztonságunkat.

Az egyik ilyen megoldás a kétfaktoros hitelesítés használata a bejelentkezéshez. A Facebook eddig is használta ezt abban az esetben, ha szokatlan bejelentkezést észlelt. Ilyen esetben a jelszó megadásán túl egy bejelentkezési kódot is küldött, amelyet szintén be kellett gépelni, így igazolva, hogy mi vagyunk a fiók jogos használója.

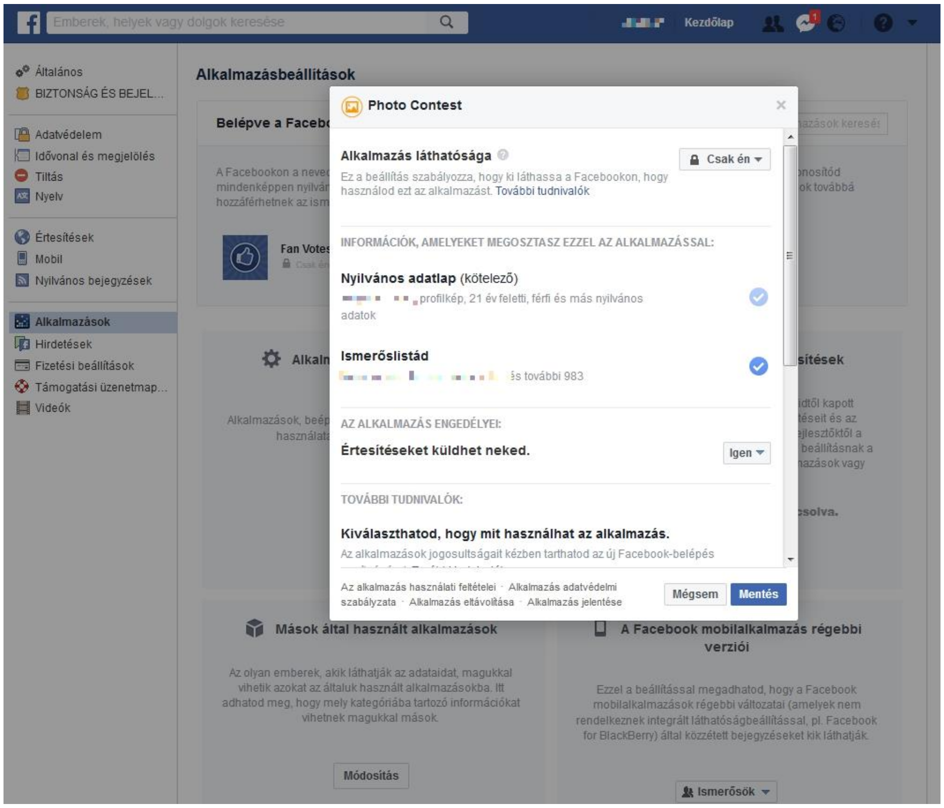
A kétfaktoros hitelesítést beállíthatjuk állandó funkcióként is, ilyenkor vagy SMS-ben, vagy valamilyen más, biztonsági hitelesítő alkalmazás (Pl. Google Athenticator vagy Duo Mobile) segítségével fogunk tudni bejelentkezni.

Érdemes megfontolnunk, hogy engedjük-e és ha igen milyen kontroll mellett, hogy mások is írjanak az idővonalunkra, vagy mások megjelölhessenek minket képeken.

A Facebookon számos olyan problémával szembesülhetünk, ami a Facebook-os alkalmazások használatából, pontosabban az alkalmazások túlzott jogosultságaiból fakad.

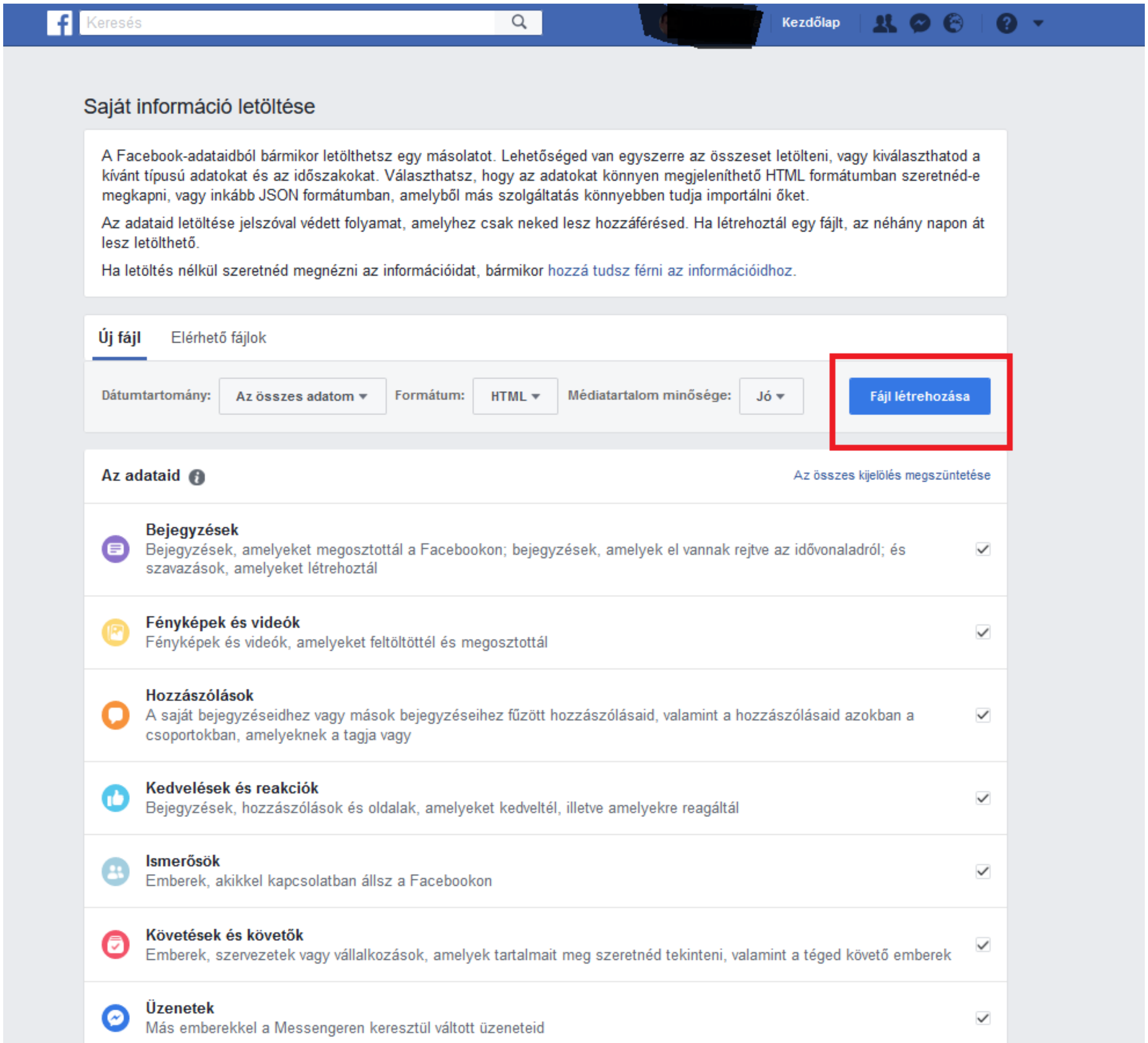
A Facebookon megtalálható alkalmazások is különböző dolgokhoz hozzá akarnak férni, például nyilvános profilunk, személyes adataink, ismerőseink, fotóink, bejelentkezett helyeink stb. Ezen kívül olyan jogosultságokkal is bírhatnak, mint például az üzenetküldés ismerőseinknek, vagy üzenetfalra írás (kvázi posztolás a felhasználó nevében). Ezek nagyon veszélyes jogosultságok, hiszen ilyenkor a felhasználó átadja a jogot az alkalmazásnak – és az alkalmazás írójának, hogy az ő nevében posztoljon, vagy írjon üzenetet. Sok esetben, ha sikerül egy ilyen jogosultságokkal bíró alkalmazást megfertőzni vírussal, akkor az pillanatok alatt terjedni kezd a Facebookon, hiszen a felhasználók azt látják, hogy jéé, milyen érdekeset írt az ismerősöm, rákattint és már ő is megfertőződött és így tovább - láncreakció szerűen.

Amennyiben használunk Facebookos alkalmazásokat időnként vizsgáljuk felül, hogy tényleg használjuk-e őket és ha nem, akkor töröljük, ha pedig igen, akkor nézzük végig, hogy mihez akar az alkalmazás hozzáférni és amit problémásnak gondolunk, azt tiltsuk le.



32. ábra Facebook alkalmazások jogosultságai

Ha tudni szeretnénk, hogy milyen adatokat és tartalmakat tárol rólunk a Facebook, akkor van lehetőségünk a tárolt adatok kategóriánkénti kijelölésére (a képernyőkép nem teljes, mivel a kategóriák több oldalon keresztül folytatódnak) és letöltésére a Beállítások menüben („A Facebook-adataid” menüpontban).



33. ábra Facebook által rólunk tárolt adatok másolatának letöltése

6.4.6.1 Nyereményjátékok és kattintásvadászat vagy lájkvadászat

A legnépszerűbb közösségi oldalon rendszeresen megjelennek olyan oldalak, amelyek valamilyen nyereményt sorsolnak ki, és mindössze annyit kérnek a felhasználóktól, hogy lájkolják az oldalt (vagy más oldalakat, lásd a képen), osszák meg és írják oda, hogy például milyen színű autót szeretnének, ha ők nyernek.

Rengetegen gondolják úgy, hogy ez a minimális erőfeszítés megéri, hiszen megadják maguknak az esélyt, hogy nyerjenek. Valójában egész más van a háttérben. Ez a

tevékenység egy nagyon egyszerű és jól jövedelmező csalási forma. Az alábbiakban leírjuk a működését.

Manapság egy jól felépített és kelendő termék vagy szolgáltatás marketing kampánya sokmillió forintba kerül és a kampány egyik célja, hogy egy termék vagy szolgáltatás Facebook oldalán minél több rajongó legyen, akiket így könnyen el lehet érni és meg lehet szólítani reklámokkal.



34. ábra Lájkvadászat hamis nyereményjátékkal

A csalók arra jöttek rá, hogy az emberek rendkívül naívak és az ingyen nyereményért bármire képesek.

A csalók létrehoznak egy Facebook oldalt, ami lehet bármilyen néven, igazából nincs jelentősége. Meghirdetnek rajta egy nyereményjátékot, ahol faházat, utazást, drága autót, bútort, ékszert, telefont, bármilyen értékes dolgot lehet nyerni. Megfigyelhető, hogy a nyereményjáték szövegezése általában helyesírási, központozási hibákat tartalmaz, ami egy magára valamit adó cég esetében nem elfogadható, ez is egy gyanús jel lehet.

A nyereményjátékban való részvétel feltétele az oldal vagy más oldalak lájkolása és megosztása. Ezzel a módszerrel napok, rosszabb esetben hetek alatt elérik, hogy a frissen létrehozott termék vagy szolgáltatásoldal többtízezer, akár százerek követővel rendelkezzen. Természetesen a nyereményjáték nem igaz, valójában nincs sorsolás és nyertes sem. A százezres követői táborral rendelkező facebook oldalt ezután a csalók eladják. Az új tulajdonos pedig átírja a nevet, lecseréli a logot és a borítóképet és máris

százezres potenciális ügyfélbázist ér el, miközben nem költött milliókat marketing kampányra.

Az embereknek meg kell érteniük, hogy milliós nyereményjátékokat jellemzően nagy cégek hirdetnek, komoly feltételekkel, a saját honlapjukon is és egyéb media felületeken is hirdetve azt. Az ilyen Facebookon terjedő nyereményjátokok jelentős része átverés és csak a csalók nyernek rajta.

6.4.7 Az adatvédelem hiányosságainak lehetséges következményei

Az adatok védelmének fontosságára világított rá a „Cambridge Analytica” néven elhíresült botrány és annak következményei. A híradások szerint egy angol-amerikai tanácsadó cég jogtalanul jutott hozzá körülbelül 90 millió Facebook-felhasználó személyes adataihoz és azokat feldolgozva – és kiegészítve legálisan vásárolt személyes adatokkal – személyre szabott politikai tartalmú üzenetekkel próbálta meg a felhasználók véleményét befolyásolni például az amerikai elnökválasztási kampány vagy az Egyesült Királyság Európai Unióból való kilépéséről szóló népszavazási kampány idején, felhasználva a „big data” elemzés és a személyes profilalkotás eszköztárát [u]. Az esemény kiderülését követően sokan törölték magukat a Facebookról és a cég az eddigi legnagyobb adatvédelmi bírságot (500.000 font) kapta. További következmény, hogy a Facebook megváltoztatta az adatvédelmi szabályozását és lehetővé tette a felhasználóknak a régebbi adatok törlését is. Az adatelemző cégtől a botrány hatására elpártoltak a megrendelői és befejezte a működését.

A Facebook számára további problémát okozhat az, hogy amerikai hírportálok szerint 61 vállalat kapott hozzáférést a felhasználók személyes adataihoz több héten keresztül, melyek jogszerűsége vitatott. Ha bebizonyosodik az adatkezelés jogszerűtlensége és a korábbi precedens lesz a bírság alapja, akkor a kártérítés összege érintettenként akár 40.000 USD is lehet, ami 90 millió sértettet feltételezve már igen komoly büntetésként jelenhet meg a cég életében [v].

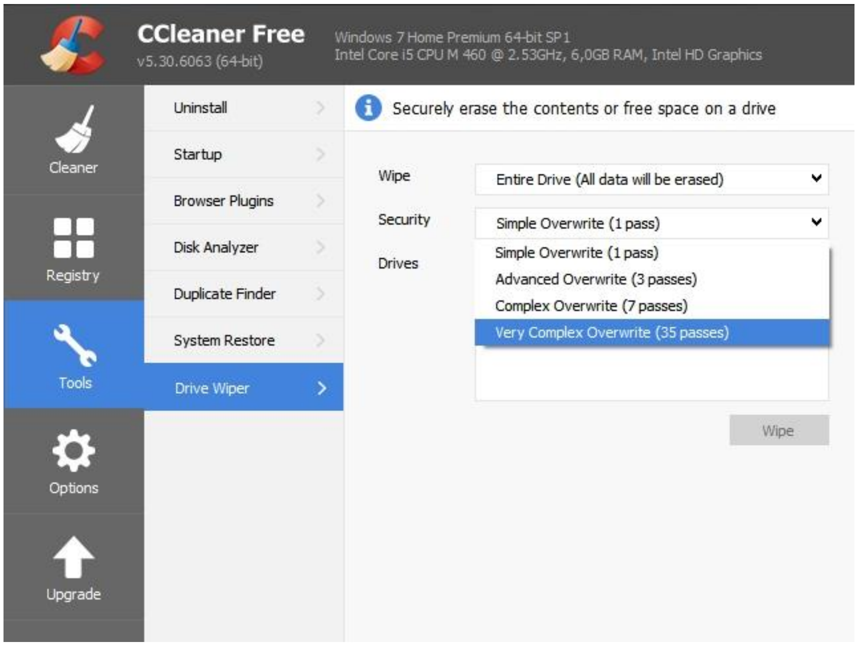
6.4.8 Az adatok végleges törlése

Az adatok visszaállíthatatlan törlésére, vagyis a **fizikai adatmegsemmisítés**re azért van szükség, hogy az adatok többé már ne legyenek visszaállíthatók, és nyugodtak lehessünk afelől, hogy a logikailag törölt adatainkban a támadók már nem kotorászhatnak értékes információk után. Erre azért van szükség, mert a számítógépes eszközökön tárolt adatokat

nem törli visszaállíthatatlanul az adatok Lomtárba mozgatása (soft delete), csupán az elérésüket, kilistázásukat szünteti meg a könyvtárban. A visszaállíthatatlan törlésre egy jó módszer az adatokat tartalmazó adathordozó (CD, DVD, pendrive, memóriakártyák) **bedarálás**a, szétroncsolása fizikailag (hard delete). Ugyanígy az adatok végleges törlését eredményezi a merevlemezek **elektromágneses törlés**e (degaussing) – ami erős mágneses mező gerjesztésével tünteti el a mágnesezett adathordozókról az adatokat, gyakorlatilag felülmágnesezi azokat – ez főleg nagyvállalati környezetben érhető tetten, otthoni felhasználók esetében a merevlemez fizikai roncsolása, átfúrása, szétszerelése és roncsolása javasolt inkább. Megfelelő lehet még a **szoftveres adatmegsemmisítő eszközök** használata is, de csak akkor, ha a célszoftverek [n] többszörös felülírás alkalmazásával teszik véglegesen olvashatatlanná a korábbi adatokat.

Fontos, hogy ma már szinte minden informatikai eszköznek van saját beépített, vagy bővíthető háttértára, amely adatokat tárol el a felhasználás során. A telefonok is rendelkeznek saját memóriával és bővíthetjük őket külső memóriakártyákkal, de ugyanez van a fényképezőgépekkel, okosTV-kel is. Fentiek miatt fokozottan oda kell figyelni arra, hogy ezen eszközök leselejtezése vagy eladása esetén meggyőződjünk arról, hogy nem maradt a háttértárakon értékes adat. Erre jó módszer lehet fent említett adatmegsemmisítő szoftver használata majd a gyári beállítások visszaállítása.

A következő ábra a CCleaner szoftvernek mutatja be azt a beállítását, amikor a merevlemez szabad területén esetleg ottmaradt korábbi adatokat 35-szörös felülírással törli – illetve teszi véglegesen elérhetetlenné.



35. ábra Végleges adattörlés szoftveresen

6.5 A sértetlenségről

Az egyes fájlok, üzenetek tárolásánál, vagy olvasásánál sokszor felmerülhet az a kérdés, hogy „vajon ezt tényleg az írta, akié az e-mailben látott e-mail cím?”. Máskor a tartalmak kérdőjeleződhetnek meg: „vajon tényleg ezt a szöveget küldte a Jóska?” Annak az eldöntésére, hogy az üzenet a küldés vagy tárolás során megváltozott-e, hitelességi eljárásokat lehetséges alkalmazni, melyek két kulcsfontosságú eleme a digitális aláírás és benne a kivonat.

6.5.1 Digitális aláírás

A digitális aláírás egy olyan titkosított kód, amely egy személy azonosságát társítja ahhoz a fájlhoz, amit aláírt, más szóval hitelesíti. A **hitelesítés** ugyanis az állított azonosság megerősítése, így a **hitelesség** az eredet és a küldő meg nem változását jelenti. A digitális aláírás szabatosabban megfogalmazva egy – aszimmetrikus kriptográfiai algoritmuson alapuló – matematikai számsor, amelynek előállítási eszköze a **digitális aláírás séma** és amely az üzenet hitelességének (eredetének és sértetlenségének) biztosítására szolgál. A digitális aláírás készítéséhez használatos aláírás-létrehozó adat (titkos kulcs) párja az aláírás-ellenőrző kulcs (nyilvános kulcs) lesz, amit a hitelesítésszolgáltatók digitális

tanúsítványba foglalnak az aláíró személy azonosítása és hitelesítése után. A digitális tanúsítvány ennél fogva igazolja, hogy az üzenet küldője valóban az, akinek állítja magát. A digitális tanúsítványok tartalmazhatnak nyilvános kulcsokat és más hitelesítő adatokat is, mint például név, város, cím, személyes azonosító adat, beosztás, szervezeti egység stb. A tanúsítványok leggyakoribb alakjai az X509v3 szerinti és a PGP tanúsítványok. Az X509v3 megjelölés a nemzetközi telekommunikációs intézet által kibocsátott X.509 szabvány harmadik verziójára utal, míg a PGP a Philip R. Zimmermann által 1991-ben készített Pretty Good Privacy [o] titkosításra és hitelesítésre készített programcsomag részeként használható digitális tanúsítványokat jelöli.

A **digitális tanúsítvány**ok különböző célokra szolgálhatnak. Vannak aláíró, titkosító, hitelesítő, személyes, szervezeti, kódaláíró és SSL-tanúsítványok is. Mindegyik tanúsítvány felépítése ugyanolyan, a különbségek az egyes adattartalmakban és a használati célokban rejlenek. Például az **SSL-tanúsítvány** – amelynek a neve a Secure Socket Layer rövidítéséből ered – arra használatos, hogy valaki az eszközeinek birtoklását hitelesítse általuk és **biztonságos kapcsolódás**t lehessen megvalósítani ennek segítségével a védett weboldallal (lásd korábban a lakat és a https). A kapcsolat azért lesz biztonságos, mert titkosított, így az illetéktelen lehallgatás ellen védett.

Az aláíró tanúsítványok digitális aláírási célra szolgálnak. A tanúsítványok tartalmazzák az aláírás-ellenőrző adatot, amelyhez tartozó aláírás-létrehozó adattal készül a digitális aláírás.

A digitális aláírás elkészítésének és fogadó oldali ellenőrzésének lépései:

- az aláírandó adatokból elkészül annak fix (általában 160–512 bit) hosszúságú kivonata,
- a kivonatot az aláíró algoritmus és a titkos kulcs segítségével rejtjelezi az alkalmazás, és ez lesz a digitális aláírás,
- az aláírás kezdeti ellenőrzése automatikusan megtörténik,
- a digitális aláírás az adatokhoz csatolva eljut a fogadóhoz.

A digitális aláírás abban különbözik a nyilvános kulcsú titkosítástól, hogy itt a titkos kulccsal történik az üzenet aláírása, a nyilvános kulccsal pedig az aláírás ellenőrzése – titkosításnál pontosan fordítva. Az aláírás elkészítése a következő lépésekben leírtak alapján történik. Az aláíró a nyílt szövegből egy kivonat- vagy lenyomatkészítő egyirányú függvénnyel (hash function) elkészíti az üzenet kivonatát. Ezt a lenyomatot kódolja a magánkulcsával, így

elkészítve a digitális aláírást. Az aláíró elküldi az eredeti kódolatlan üzenetet és az üzenetből készített kódolt lenyomatot.

Az aláírás ellenőrzését az aláírás létrehozása után a megfelelő információk birtokában utólag is el lehet végezni.

Emlékeztetve arra, hogy az aláírás készítésének utolsó lépéseként a küldő a digitális aláírást az adatokhoz csatolva eljuttatja azt a fogadóhoz, a fogadó az alábbi módon, utólagosan így ellenőrzi az aláírást:

- a fogadó az adatokból elkészít egy új kivonatot,
- a digitális aláírásból a nyilvános kulcs segítségével visszaállítja az eredeti kivonatot,
- a fogadó az új kivonatot és az eredeti kivonatot összehasonlítja, és ha egyezik, akkor az aláírás rendben van, ha nem egyezik, akkor pedig az aláírás elfogadását – alapesetben – megtagadja.

A digitális aláírás sikeres ellenőrzéséből az alábbiak következnek:

- az aláírt adatok ugyanazok, amit a küldő elküldött, menet közben nem változtak,
- az adatok aláírását a nyilvános kulcshoz tartozó titkos kulccsal végezték, és
- amennyiben a nyilvános kulcshoz létezik tanúsítvány, és tanúsítványban szereplő névhez tartozó személyt megbízható módon kapcsolták, akkor az a fizikai személy is ismert, aki aláírta az adatokat.

A digitális aláírás ellenőrzésének sikertelensége esetén az alábbiak lehetnek – a teljesség igénye nélkül – az okok:

- az adatok a küldés során megváltoztak,
- az ellenőrzéskor más kulcsot vagy algoritmust használtak,
- a tanúsítványt nem tette a fogadó még megbízhatóvá a saját rendszerében,
- a tanúsítvány lejárt,
- a nyilvános kulcshoz tartozó tanúsítvány hibás.

Az ellenőrzés sikertelensége okán kapott hibaüzenet behatárolhatja a hiba pontos okát, ami segít az aláírás ellenőrzésének sikeres megvalósításában. A megfontolt és körültekintő eljárás indokolt, mivel az érvénytelen aláírás elfogadásából adódó minden következmény az elfogadót terheli.

Hol alkalmazzák ezt a technológiát elsősorban? A programozók a fejlesztett kódokat alá szokták írni ma már digitálisan, hogy a támadók addig se tudják észrevétlen módosítani ezeket a tartalmakat, amíg eljutnak a felhasználók gépeire (kódaláírás). A telepítések előtt érdemes elolvasni azt az üzenetet, mely megmutatja a telepítendő szoftver íróját is. Másrészről a teljesen elektronikus ügyintézés nem képzelhető el másként, csak digitális aláírással, hiszen így tud meggyőződni az ügyintéző a beküldött nyomtatvány aláírójának személyazonosságáról anélkül, hogy az ügyfél személyesen is megjelenne előtte, továbbá így lehet biztosítani az ügyintézés során rögzített adatok hosszú távú hitelességét is a legegyszerűbben. Ilyen ügyintézési terület ma Magyarországon például a cégeljárás. Nemzeti és nemzetek feletti közösségek más területeken is használják már ezt a technológiát, azonban globális alkalmazása egyelőre nem megoldott [p].

6.5.2 Kivonatok (hash-ek)

A digitális aláírások készítésénél felmerült az a probléma, hogy elviekben a digitálisan aláírandó fájlok mérete nem korlátos, illetve jelentős eltéréseket is mutathat (pár bájttól pár/sok terrabájtig is akár), így a hatékony aláíráskészítéshez szükségessé vált egy olyan eljárás közbeiktatása, mely az aláírandó adat méretétől függetlenítette az aláírási algoritmust – így őrizve meg annak hatékonyságát és alkalmazhatóságát. Ez az eljárás tetszőleges bináris adathoz egy fix hosszúságú bitsorozatot rendel egyedileg hozzá, amit az adat lenyomatának, kivonatának vagy - az angol szót átvéve - hash-ének nevezünk.

A digitális aláírásoknál felhasználható, "jó" kivonatoló, azaz hash algoritmusok az alábbi matematikai tulajdonságokkal rendelkeznek - emiatt lesznek alkalmasak a hosszú távú, biztonságos használatra:

- Egyirányúság (pre-image resistance): ha egy adott üzenet hash értékét ismerjük csupán, akkor ebből gyakorlatilag lehetetlen legyen az üzenetet visszafejteni. Ha ez a tulajdonsága nem lenne, az aláírásokhoz utólag is lehetne üzenetet készíteni. Ez esetben nem lehetne az üzenet megváltozását felderíteni.
- Lavina-hatás (2nd pre-image resistance): adott kivonathoz és üzenethez gyakorlatilag lehetetlen olyan az eredeti üzenettől különböző másik üzenetet találni, amelyeknek a kivonata megegyezne. Más szóval, ha bármely két üzenetet tekintünk - például tekintsünk egy szó kivételével teljesen azonos két üzenetet, a kivonat értékeinek (jelentős mértékben) különbözőnek kell lenniük. Az aláírásoknál ez a tulajdonság ott lesz fontos, hogy ne lehessen ugyanazt az aláírást felhasználni egy teljesen más (például a támadó által készített) üzenethez.

- Ütközés-mentesség (collision resistance): gyakorlatilag lehetetlen két olyan üzenetet találni a lehetséges üzenetek halmazában, melyeknek a kivonata megegyezik. Ez a tulajdonság fogja megvédeni az aláírást az előre megválasztott üzenetek típusú támadásoktól - amikor a támadó az előre elküldött üzenetet íratja alá, de az általa másodikként megtalált üzenetre cserélné ki az aláírt üzenetet. Erre az üzenetek halmaza és a lehetséges hash értékek halmaza méretének lényeges (sok-sok nagyságrendnyi) különbözősége ad lehetőséget.

6.6 A rendelkezésre állás megteremtése

A rendelkezésre állás megteremtése a gyakorlatban négy dolog biztosítását jelenti – hálózati környezetben:

- áramellátás a hardver számára
- adatok és szoftverek az alkalmazások számára
- hálózati sávszélesség biztosítása az elérhetőség érdekében
- végpontvédelem a működésbiztonság megőrzése számára

Az áramellátást szünetmentes tápegységek [q] alkalmazásával tudjuk biztosítani – léteznek otthoni és ipari méretű eszközök is, egyszerűen beszerezhetők és telepíthetők. Időnként – az akkumulátorok elhasználódása miatt – cserére szorulnak, egyébként más többletfeladatot nem jelentenek és hatékonyan védik a számítástechnikai eszközöket az áramellátás meghibásodásaitól.

A hálózati sávszélességben három tényező játszik szerepet:

- mekkora sávszélességre fizettünk elő a szolgáltatónál
- mennyi a valós felhasználási igényünk
- mennyire van védve a hálózat a szolgáltatás-megtagadásos támadások ellen (DoS, Denial of Service)

A **DoS-támadás**ok kivitelezésekor a támadók valódinak látszó kérésekkel, de hibás, vagy módosított adatcsomagokkal bombázzák egy időben a szervert. De nem foglalkoznak a válaszokkal, mert a cél a folyamatos kérésekkel a szervert annyira leterhelni, hogy más felhasználók kérésének feldolgozására a szervernek ne maradjon kapacitása, így az lelassul a külső szemlélő számára, vagy megszűnik válaszolni. A leterhelés hatványozottan sikerülhet, ha hibás az adatcsomag és a szerver oldalnak több idő feldolgozni vagy mondjuk egy-egy hibás feldolgozásnál végtelen ciklusba kerül. Otthoni felhasználóknak jó

hír, hogy az erre irányuló védelem megteremtése a szolgáltató feladata és nem is jellemző, hogy felhasználói gépeket támadjanak így. Sokkal gyakoribb, hogy nagyobb internetes szolgáltatásokat (közösségi oldalak, webáruházak, kormányzati szolgáltatások vagy egyéb egyedi célpontok) próbálnak meg elérhetetlenné tenni valamilyen politikai vagy egyéb érdekből, illetve zsarolási szándékkal.

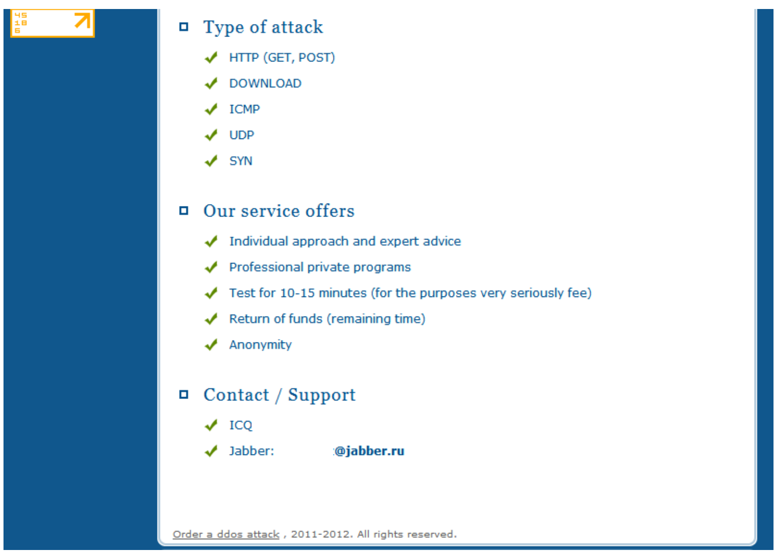
A DoS támadásoknak van egy erősebb változata a dDoS (distributed Denial of Service). Ezt a típusú támadást egy időben egyszerre több ezer, százezer, vagy millió gépről is indíthatja a támadó (akár megfertőzött okoseszközökről is). Felmerül a kérdés, hogy ki rendelkezik egyszerre mondjuk egymillió számítógép felett irányítási joggal? Ma már egyre több olyan bűnszervezet létezik, akik az otthoni felhasználók millióinak számítógépét és okoseszközeit megfertőzik trójai programokkal, amelyekkel át tudják venni felettük az irányítást a felhasználó tudta nélkül. Az ilyen módon összekapcsolt számítógépek hálózatát botnetnek (roBOT és NETwork szavakból alkotva) hívjuk. Az ilyen botneteket a támadók sokszor bérbe adják az internet sötét oldalán, a bérlők pedig arra használják ezeket a gépeket, amire akarják. dDoS támadás, SPAM küldés, jelszótörés és még számos illegális tevékenység felsorolható lenne itt. A rossz hír, hogy ilyen botneteket nem csak számítógépekből, hanem okoseszközökből (telefonok, okosTV-k, IP kamerák, okosotthon vezérlő számítógépek) is építenek már a támadók. Ennek ellenére az okoseszközök védelmével a felhasználók és a gyártók még nem kielégítően foglalkoznak, pedig fontos lenne.

Dos és dDoS támadások eredményeként a megtámadott internetes szolgáltatás nem lesz elérhető. Ha valakinek az üzleti működése múlik egy honlapon, akkor érdemes felkészülni egy ilyen támadásra. Hiszen ha nem elérhető a webáruház például, akkor nincs bevétel.

Az alábbiakban egy olyan felületet látunk, ahol egy dDoS támadáshoz lehet bérelni felhasználók megfertőzött számítógépeit, kiiktatva például az internetes konkurenciát. Fontos tudni, hogy az ilyen szolgáltatások használata is törvénybe ütközik!



36. ábra dDOS támadás megrendelő felület 1. rész



37. ábra dDOS támadás megrendelő felület 2. rész



38. ábra dDOS támadás megrendelő felület 3. rész

Ha egy szolgáltatás nem elérhető, vagy egy hacker feltörte a szolgáltatásunkat és adatokat törölt, akkor felvetődik az a kérdés, hogy hogyan lehetséges a szükséges információkat, programokat, alkalmazásokat úgy lementeni, hogy szükség esetén a lehető legrövidebb időn belül vissza lehessen őket tölteni, és újra a rendelkezésünkre álljanak. A digitális világ fejlődésével egyre több adat már csak elektronikusan készül és tárolódik, akár otthon, akár a munkahelyen vagyunk. A leggyakoribb hiba, amit el szoktak követni az, ha az adatnak csak egyetlen egy példánya keletkezik és nem készítenek róla másolatokat, **mentés**eket. A hardver meghibásodása (merevelemez olvasófej, mágneslemez felülete, mágnesezettség), vagy az eszköz (telefon, laptop) elveszése, ellopása következtében ezek az adatok megsérülhetnek, megsemmisülhetnek annyira, hogy részleges vagy teljes visszaállításukra sem lesz lehetőségünk.

6.6.1 Fájlok biztonsági mentése

Az adataink a számítógépben fájlokban tárolódnak, emiatt az egyes fájlok rendelkezésre állásának biztosítása ezeknek a fájloknak a mentését jelenti.

Az adatvesztés ellen az adatok megőrzése, a mentések létezése nyújthat egyedül védelmet, tekintettel arra, hogy az újra előállításuk sok esetben problémákba ütközik. A mentések tervezésénél az alábbiakat kell megfontolás tárgyává tennünk:

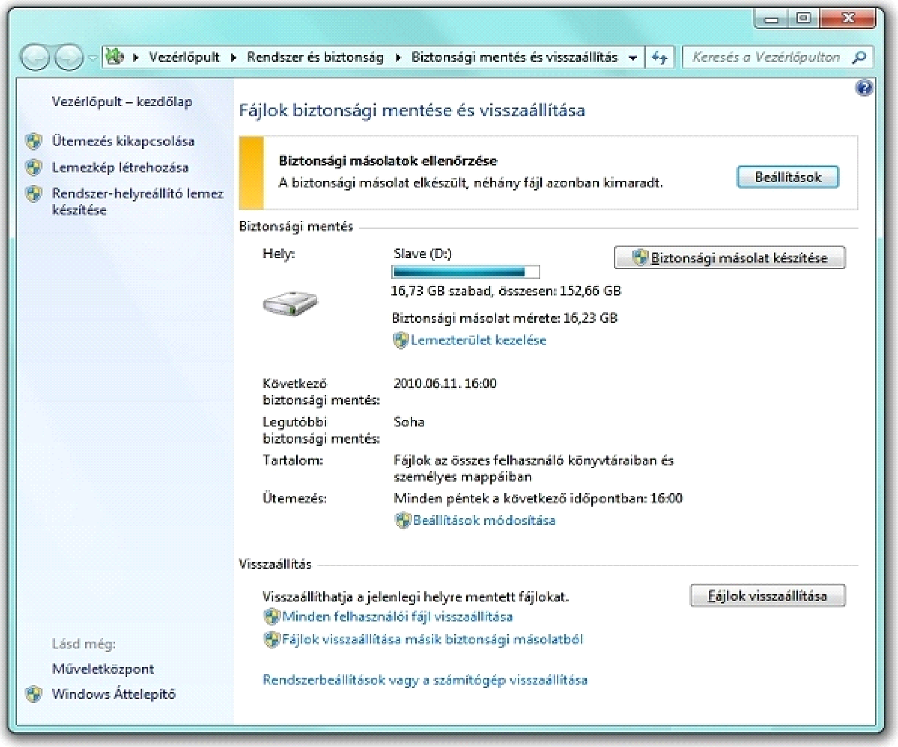
- Mekkora adatmennyiséget kell mentenünk?

- Milyen gyakran változnak meg a mentendő adatok? Milyen gyakran kell elmenteni őket ahhoz, hogy lehetőleg ne legyen súlyos adatvesztés?
- Hány példányban kell a mentést elvégezni?
- Mikor kell a mentést elvégezni, más szóval mikorra lehetséges ütemezni a mentést ahhoz, hogy ne zavarjon senkit sem?
- Meddig kell megőrizni a mentéseket?
- Hol tároljuk a mentéseket?
- Hogyan kell a mentéseket biztonságosan megsemmisíteni?

Windows rendszerben a mentést a beépített automatikus biztonsági mentési eszköz, a Windows Backup [r] biztosítja a legegyszerűbb módon. A Windows backup a teljes rendszert lementi olyan formában, hogy egy visszaállítás után a működés ettől a ponttól fog újraindulni. Tekintettel arra, hogy ez a módszer a teljes rendszert, szoftvereket, adatokat, konfigurációkat is lementi, ezért nagy helyigénnyel rendelkezhet – emiatt sűrű használata nem célszerű ritkán megváltozó adatok esetében.

A teljes rendszer mentése helyett hatékonyabb megoldás az egyes fájlok, vagy könyvtárak mentése, amit különböző segédprogramok támogatnak. Ilyen eszköz például az Ubuntu Linuxra fejlesztett Time Vault [s] alkalmazás is. Az egyes könyvtárak vagy fájlok kijelölése után a pillanatfelvétel egy gombnyomásra elkészíthető. A fájlok elnevezése hatással lehet olykor a mentés sikerességére, mivel a nagyon **bonyolult fájlnevek** (ékezetes betűk, különleges karakterek, mély könyvtárstruktúra) mentésére nem minden program van felkészülve. Kevésbé hatékony megoldás lehet a fájlok manuális másolása, például egy külső merevlemezre, vagy egy nem állandó jelleggel felcsatlakoztatott felhő alapú tárhelyre – de a semminél még ez is jobb megoldás.

Fontos, hogy a mentési adathordozók ne legyenek állandóan a számítógéphez csatlakoztatva (vagy ha felhő alapú, akkor állandóan felcsatolva), mivel egy vírustámadás során a mentésünk is érintett lehet és akkor nem sok értelme volt az egésznek. A másik ok, amiért nem szabad a mentéseknek fizikailag a mentett gép mellett lenni az az, hogy ha esetleg a gépet ellopják, vagy leég, vagy egyéb fizikai behatás miatt tönkre megy, akkor a mellette tárolt mentésünk is ugyanezt a kárt fogja elszenvedni. Érdemes időnként a fizikai mentés egy-egy példányát más helyszínre szállítani és ott tárolni. A cégek erre a célra vagy egy földrajzilag távoli és jól védett telephelyüket vagy bankok széfjeit szokták használni.



39. ábra Windows Backup

A visszatöltés is egyszerűen elvégezhető egy kattintással, de javasolt a mentéseket másik lemezre vagy fizikailag védett médiára végezni – amit biztonságos háttér-adattárolónak nevezünk, hogy ne az eredetivel együtt sérüljenek meg.

Az okostelefonok használata során nagyon sokan elfeledkeznek arról, hogy ezeken az eszközökön is rengeteg fontos adatot tárolunk. Telefonszámok és egyéb kontakt adatok, SMS-ek, fényképek, feljegyzések, kimutatások, videók. Gondoskodni kell az okostelefonok adatainak mentéséről is. Erre szintén vannak célszoftverek, különböző funkcionalitással.



40. ábra Okostelefonok fontos adatainak mentése



41. ábra Adatok mentése Windows környezetben (Aomei backup))

A mentések gyakoriságát úgy válasszuk meg, hogy egyrészről ne jelentsen többlet terhet, másrészről az utolsó mentés és a hiba bekövetkezése közötti időben keletkezett adatok pótlására is legyen reális lehetőség – vagy a hiányuknak ne legyen különösebb következménye. A mentések példányszámának kialakítása során vegyük figyelembe, hogy több mentés nagyobb biztonságot jelent ugyan, de többletfeladatot ró ránk a selejtezésük

és a bizalmasság terén is lépnünk kell (pl. mentések titkosítása) azért, hogy a mentett adataink bizalmassága is megmaradjon, hasonlóan az eredeti adatok bizalmasságához (az egyenszilárdság miatt).

6.6.2 Védelem az áramellátás hibái ellen

A szünetmentes áramellátó berendezések használata számítástechnikai és ipari környezetben, vagyis otthon és a munkahelyen ma már elengedhetetlenné vált. Nem szívesen vállaljuk fel ugyanis egy áramszünet, illetve a feszültségingadozással járó zavarok hátrányos, költséges következményeit. Az **elektromos hálózat**ról üzemeltetett eszközök működése függ a hálózat működésétől, más szóval attól, hogy van-e áram. Az otthoni eszközök java része kizárólag az elektromos hálózatról működik, amely meghibásodása esetén károsodásokat szenvedhetnek. Az ilyen károk megelőzhetők és elkerülhetők akkumulátoros háttérrel rendelkező szünetmentes áramforrások alkalmazásával. A szünetmentes áramforrások ára és fenntartási költsége általában jóval kisebb, mint az a kárösszeg, melyet az áramszünetek és a hálózati áramellátás ingadozásai, túlfeszültségei okozhatnak.

A hordozható számítógépek akkumulátorai valameddig védelmet nyújtanak az áramkimaradás és az esetleges ingadozások ellen, de az asztali gépeknek nincs ilyen védelmük, így egy áramellátási incidenst működési zavar, meghibásodás is követhet. Ha a hálózati eszközöket nem védjük szünetmentes tápegységgel, akkor bár a számítógépünk működni fog, de nem érjük el az internetet a szokásos módon. Az otthoni védelemre példa az alábbi kis teljesítményű és méretű szünetmentes áramellátást biztosító egység.



42. ábra Szünetmentes otthoni áramellátó eszköz

6.7 Komplex megközelítést igénylő fenyegetettségek és védelmi megoldások

6.7.1 Végpontvédelem és vírusvédelem

A számítástechnika és az internet kezdetekor is az első komoly, minden felhasználót érintő probléma a vírusok megjelenése volt, amit kezdetben unatkozó programozók készítettek szórakozásból, majd egy komoly evolúción keresztül eljutottak odáig, hogy ma már kiberfegyverekként emlegetik őket és az internetes bűnözés egyik fő bevételi forrását jelentik. Felhasználói oldalról ezért az egyik legfontosabb komplex védelmi intézkedés a saját számítógépünk, okostelefonunk védelme. Míg korábban egy szimpla vírusvédelmi program is elegendő volt, addig ma már az összetett támadások ellen hasonlóan komplex, többféle fenyegetéstől is megóvó végpontvédelemre van szükség.

6.7.1.1 Vírusvédelem

A vírusirtó szoftverek alkalmazása a legismertebb és legjellemzőbben elterjedt védekezési módszer, hatékonyan véd a **fertőzések** ellen. Az okostelefonok esetében a felhasználók jelentős része még nem gondolja úgy, hogy a számítógépéhez hasonló szintű védelemről kell gondoskodnia, pedig nagyon indokolt lenne. Szinte minden vírusvédelemmel foglalkozó szoftvergyártónak van kifejezetten okostelefonokra készített víruscédelmi program verziója. Ezek közül vannak ingyenesek, fizetősek is. A lényeg, hogy legyen védelem az eszközünkön! Vírusvédelmi programokat, hasonlóan más alkalmazásokhoz, az adott platform alkalmazás áruházából tudunk letölteni illetve megvásárolni. A fizetős vírusirtókra is igaz a bővebb funkcionalitás, a gyártói támogatás biztosítása.

Fontos, hogy a telefonunkon használt ingyenes programok esetén a reklámok között felbukkanhatnak a telefonunk fertőzöttségével riogató és magukat vírusvédelmi programnak álcázó kártevők letöltésére ösztönző felugró ablakok, figyelmeztetések. Ne dőljünk be ezeknek, mivel ezek a programok maguk a kártevők! Összefoglalva, legyen egy saját, valamilyen neves gyártó által készített vírusirtó program a telefonunkon, amiben megbízunk!

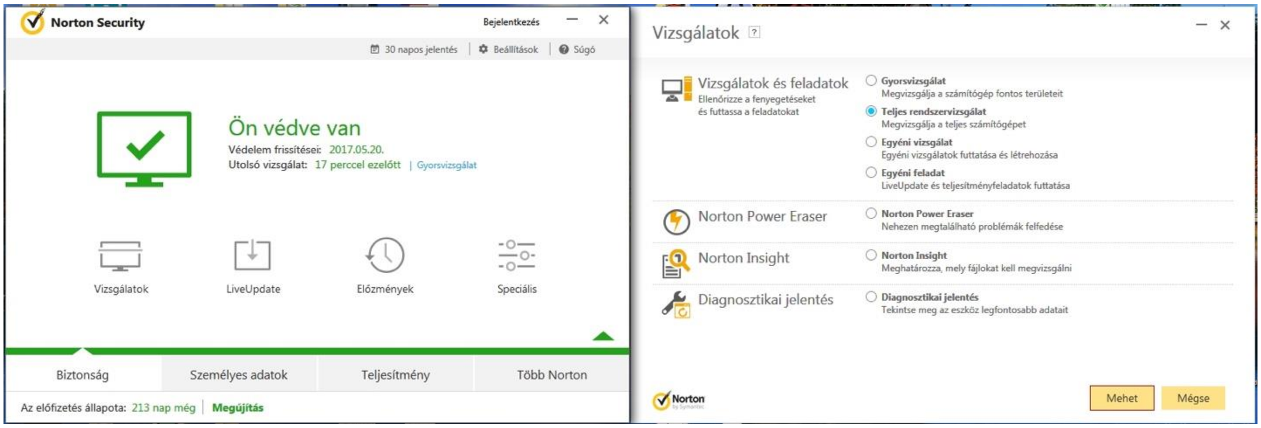
A fertőzés szó alatt számítógépes vírusok esetében egy speciális rosszindulatú program operációs rendszerbeli fájlokhoz való hozzákapcsolódását értjük. A vírusirtó programok több lehetőséget ajánlanak fel a fertőzött fájlok kezelésére, a megjelöléstől a karanténba helyezésen át a végleges törlésig terjednek a **fertőzésmentesítés** eszközei.

A **karantén** az operációs rendszerben egy olyan zárt tárolóterületet jelöl, amelyben a rendszer nem engedélyezi a programok aktív tevékenységét, futását. A karanténban lévő

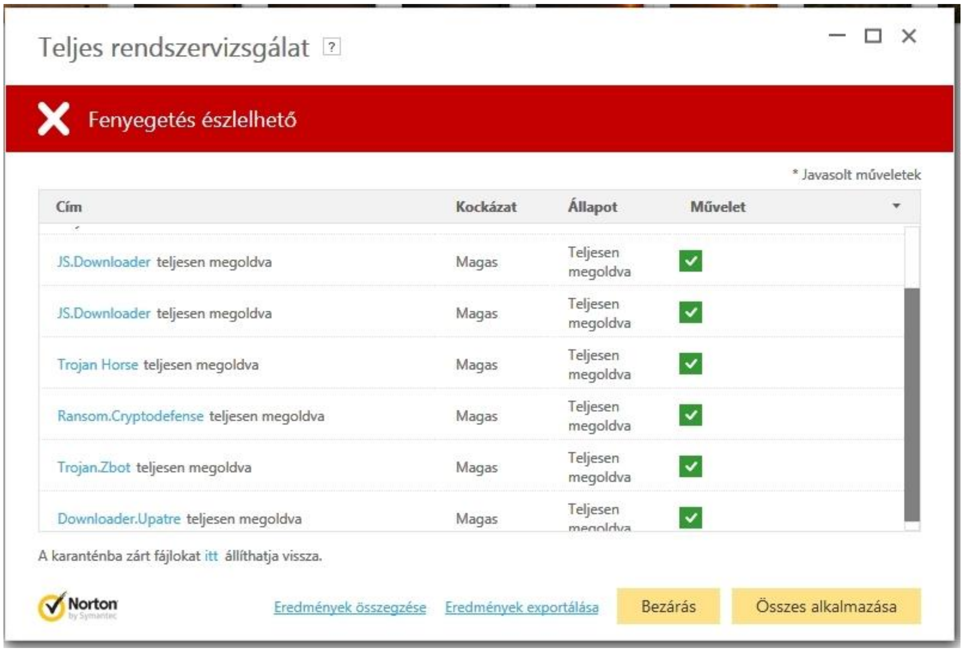
fájlok visszaállíthatók, ha ez éppen szükségessé válik, de ezt csak nagyon indokolt esetben javasolt megtenni. A karanténba zárás legfontosabb indoka ugyanis az, hogy ezeket a programokat el kell a működési környezettől különíteni, mert nem lehet őket fertőzés-mentesíteni, így nem tudjuk megszabadítani a gépet károkozóktól, mert valamiért a vírusirtó program erre nem képes.

Minden vírusirtónak van egy állandóan működő része, ami az aktuális forgalmat szűri és különböző módszerekkel történő vizsgálatokat követően nem engedi be a gyanús, vagy potenciálisan fertőzött fájlokat, illetve különböző mélységű ütemezett kereséseket is végre tudnak hajtani, leginkább üresjárati időpontokban. Ezeket a felismeréseket egyrészt a vírusdefiníciós fájlban tárolt mintákkal való összehasonlítás teszi lehetővé, másrészt egyre elterjedtebb a reputáció alapú vizsgálat, amikor a vizsgált fájl tulajdonságai alapján ellenőrzi a program, hogy valahol máshol a világban ugyanerre a fájlra volt-e már riasztás vagy egyéb negatív tapasztalat. Azért, hogy a legújabb vírusok ellen is védettek legyünk, rendszeres időközönként javasolt a vírusdefiníciós fájlokat letölteni és frissíteni a víruskereső motor verzióját is. Jellemzően ezek a funkciók már automatikusan, naponta akár többször is elindulnak.

Célszerű legalább heti rendszerességgel úgynevezett „Teljes rendszervizsgálatot” végrehajtani. Ilyenkor a vírusirtó program a számítógépen/okostelefonon lévő összes fájlt (beleértve a számítógéphez csatlakoztatott külső tárhelyeket is) átvizsgálja kártevők után kutatva. A heti rendszerességnek az ad indokoltságot, hogy egyre elterjedtebbek az úgynevezett nulladik napi sérülékenységeket kihasználó kártevők. A támadók az alkalmazott eszközeikből fakadóan olyan gyorsan tudják mutálni és kiküldeni, terjeszteni a kártevőket (pl. spam levelekben), hogy a legfrissebb vírusminta adatbázissal rendelkező program sem fogja felismerni ezeket, mert túl kicsi az az időablak, amíg a vírus elkészül, kiküldik millió számban, majd eljut a vírusvédelmi gyártókhoz, akik feldolgozzák, majd kiadják az újabb mintákat és azok elkerülnek a felhasználók vírusvédelmi szoftvereibe. Ezért lehetnek olyan levelek, fájlok, amelyek átjutottak a szűrésen és csak később két három nap, vagy akár egy hét múlva talál rájuk a teljes keresés.



43. ábra Teljes rendszervizsgálat Norton Security programmal



44. ábra Teljes rendszervizsgálat eredménye, ha vírusos a vizsgált számítógép

A vírusirtó szoftvereknek – mint minden védelmi intézkedésnek – vannak előnyei és hátrányai is. Előnye a vírusirtóknak, hogy felismerik a vírusokat a számítógépen, illetve megvizsgálják a számítógépet, hogy nem fertőződött-e meg. A vírusirtó szoftverek nagyon erős korlátja az, hogy a tényleges védettség fenntartásához naprakészen kell tartani a vírusdefiníciós fájlokat, ami rendszeres internet-kapcsolatot és frissítési tevékenységeket igényel. Elavult vírusdefinícióval hamis biztonságtudat alakulhat ki, ami szintén egy kockázati lehetőség.

6.7.1.2 Végpontvédelem

A végpontvédelem annyival nyújt többet az egyszerű vírusvédelemnél, hogy a komplex végpontvédelmi megoldások tartalmaznak személyi tűzfalat, behatolás-detektálást, spam védelmet, szülői felügyeleti lehetőségeket és végül, de nem utolsósorban, beépülve a böngészőkbe a böngészés során érkező fenyegetettségektől védenek (védelem adathalászat ellen, weboldalak biztonsági értékelése). Minden neves gyártónak van ilyen csomagja, általában „Internet Security csomag” név alatt érhetők el.

Nem mehetünk el szó nélkül az egyre elterjedtebb okostelefonok védelme mellett sem. Az okostelefonok is ugyanúgy számítógépek, mint nagyobb társaik épp ezért ugyanúgy fenyegetettek, mint az asztali munkaállomások vagy laptopok. Okostelefonokra is elérhetőek végpontvédelmi megoldások – fizetősek és ingyenesek egyaránt. Rengeteg olyan kártevő program van – és számuk rohamosan nő, amelyeket a legelterjedtebb okostelefon platformra az Androidra írtak meg. Természetesen nem kivétel a Windows és az iOS platform sem ezalól. Az okostelefonok szinte éjjel-nappal online vannak, elérik az internetet – és ezzel együtt ezek az eszközök is elérhetők az internet felől. Ugyanúgy meg tudnak fertőződni, mint a PC-k, ugyanúgy le tudja titkosítani a tartalmukat egy zsarolóvírus és ugyanúgy botnet hálózat részei lehetnek, ha a támadóknak sikerül az okostelefont megfertőzni. Figyelni kell ugyanakkor az ingyenes programok reklámjaiban felbukkanó és azonnal fertőzéssel riogató hamis vírusvédelmi programokra is. Lehetőleg valamilyen neves gyártó alkalmazását töltsük le a hivatalos forrásokból (Google Play, AppStore, Windows Central) és használjuk rendszeresen ugyanúgy, mint a hordozható vagy asztali számítógépeinken (frissítések, online ellenőrzés, rendszeres teljes keresés).

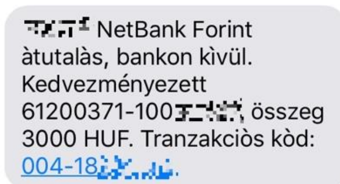
6.7.2 Biztonságos Internet bankolás

Manapság egyre elterjedtebb az internetes bankszámlakezelés. A bankok mindent megtesznek azért, hogy az e-banki szolgáltatásaik megfelelően védettek legyenek és védelmet nyújtsanak az ügyfelek adatai számára is. Egyrészt ez saját üzleti érdekük, másrészt a Pénzügyi Felügyelet is szigorúan ellenőrzi a bankok által megtett erőfeszítéseket.

Az internetes bankolás a felhasználói oldalról megvizsgálva két kritikus pontot hordoz. Az egyik a belépés, a másik a különböző pénzügyi műveletek végrehajtása.

Az internetbanki belépésre a hazai bankok évek óta kínálnak megerősített, úgynevezett kétfaktoros bejelentkezést. Ilyen lehet az SMS-ben érkező egyszerhasználatos jelszó, a

bank által adott hardveres véletlenszám generátor (token), illetve a chipkártyás beléptetés. Vannak bankok, ahol ezek a megerősített belépési módok nem kötelezők, de választhatók. Ahhoz, hogy az ügyfeleket ne érje kár, ne lehessen a pénzüket jogosulatlanul ellopnia egy támadónak, a bankok a különböző tranzakciókat már kötelező jelleggel, csak valamilyen többfaktoros módszerrel megerősítve fogadják be. Legegyszerűbb példa lehet erre egy utalás, ahol a beküldött megbízást követően egy megerősítő tranzakciós kódot küld a bank. Az SMS-ben benne van a célszámla, az utalandó összeg és a legvégén a tranzakciós kód is.



45. ábra Tranzakció hitelesítő SMS üzenet

Mivel ez minden esetben a felhasználó telefonszámára érkezik meg, még ha egy támadónak sikerült is belépnie a felhasználó netbankjába, ha az utaláshoz szükséges tranzakciókódot nem adja meg az ügyfél – mert feltűnik neki, hogy nem ő akart utalni, vagy nem oda, nem ekkora összeget, akkor a tranzakció nem fog létrejönni, nem lesz anyagi veszteség. Ha ilyet tapasztalunk, akkor azonnal értesítsük bankunkat és várjuk meg, amíg megvizsgálják bejelentésünket. A bizonyítottan téves vagy jogosulatlan tranzakciók rendezésére jogszabály kötelezi a pénzintézeteket.

Annak érdekében, hogy a felhasználó internetes bankoláshoz szükséges adatait ne lehessen ellopni és az ügyfelek felkészültek legyenek az ilyen típusú támadások ellen, minden bank a weboldalán biztonsági figyelmeztetéseket tesz közzé, amit érdemes megfogadni és alkalmazni.

6.7.3 Biztonságos bankkártya használat – internetes fizetés

6.7.3.1 Kártyahasználat

A bankkártya egy olyan készpénzfizetést helyettesítő eszköz, melyet a bank ad(hat) a nála számlát vezető ügyfeleinek. Szinte mindegyik bankszámlához kapcsolódhat valamilyen típusú bankkártya. Használatával lehetőség van vásárolni és ATM-ekben készpénzt felvenni. (Forrás: www.bankracio.hu)

Fontos, hogy a bankkártyán fizikailag leolvasható adatok (16 jegyű kártyaszám, lejárat, név, kibocsátó bank, hátul pedig a háromjegyű ellenőrző kód (CVC/CVV2)) a mágnescsíkon és a chipben is el vannak tárolva. Egy dolog nincs eltárolva, az a PIN kód.

Ha egy fizikailag is létező boltban fizetünk a kártyánkkal, vagy pénzt veszünk fel az ATM-ből, akkor fizikailag jelen kell lennie a kártyánknak és jellemzően tudni kell a kártyához tartozó PIN kódot. Éppen ezért nem szabad a PIN kódot felírni és a pénztárcánkban a kártya mellett tárolni, még kevésbé szabad a kártyára ráírni. A PIN kód begépelésénél ügyeljünk arra, hogy ne lássák illetéktelenek a beírt kódot. Amennyiben lehetőségünk van megválasztani PIN kódunkat, akkor lehetőleg bonyolítsuk meg, ne a legegyszerűbb 1111 vagy 1234, illetve az ehhez hasonló kódokat válasszuk.

ATM készpénzfelételnél mindig győződjünk meg arról, hogy a kártyabeadó nyílásra nem helyeztek-e rá egy kártyamásoló eszközt. Ezt a kártyabeadó nyílás (csőr) finom megmozgatásával tudjuk ellenőrizni. Ha bármi gyanúsat tapasztalunk, például nem villog a csőr, vagy ragasztónyomokat látunk a szélén, akkor ne használjuk a kártyánkat, hanem azonnal értesítsük a bankot vagy az ATM üzemeltetőjét az automatán található telefonszámon.



46. ábra Kártyamásoló eszköz ATM-en

Hasonlóan ellenőrizzük le a PIN billentyűzetet. Ott, ahol kártyamásolás van, a PIN kódot is el szeretnék lopni a támadók. Erre vagy rejtett kamerát használnak, vagy a PIN

billentyűzetre rátesznek egy másik billentyűzetet, amelyen ha az áldozat megadja a kódját, így az máris a támadók birtokába kerül.

Internetes fizetéshez nem szükséges a kártya fizikai jelenléte, elegendő, ha a kártyán szereplő adatokat ismerjük. Éppen ezért fontos, hogy amikor fizikailag fizetünk a kártyával, ne engedjük, hogy elvigyék, ne tévesszük szem elől, mert ez idő alatt lefotózhatják a kártyát és máris megvannak az adatok. A modern NFC technológiával ellátott kártyák esetében nem kell kiadni a kártyát a kezünkből, elég, ha odaérintjük a terminálhoz.

6.7.3.2 Biztonságos internetes fizetés

A világban egyre elterjedtebb az online vásárlás. A különböző webáruházakban megvásárolt termékek esetében választhatjuk az utánvétes fizetést, de a leggyakrabban valamilyen elektronikus fizetési megoldást használnak az ügyfelek. Az elektronikus fizetési eljárások mögött jellemzően egy elektronikus bankszámla áll, amihez egy vagy több bankkártya is kapcsolódhat.

Érdemes olyan megbízható webáruházakat használni, ahol nem a webáruház kezeli a kártyánk adatait, hanem átirányít a bank fizetési oldalára, ott megtörténik a kártyás fizetés, majd a kereskedő megkapja az értesítést a fizetésről, mi pedig megkapjuk az árut vagy szolgáltatást.

Több bank kínál kifejezetten internetes fizetésekhez úgynevezett virtuális kártyát. Ez a megoldás azért jó, mert a kártya fizikailag vagy nem létezik, vagy ha igen, akkor sincs rajta sem mágnescsík, sem chip, tehát készpénzfelvételre vagy POS terminálos fizetésre nem alkalmas. Csak a kártyaadatok érdekesek. A virtuális kártya általában vagy a főszámlánkhoz kapcsolódik vagy saját alszámlával rendelkezik. Amikor használni szeretnénk a kártyát, akkor előzetesen fel kell a kártyalimiteket (összeg és használati darabszám) emelni (Telebank, Internetbank), amelyek vagy közvetlenül a vásárlás után vagy időzáras limitnél 24 vagy 48 óra után visszaállnak az alaplimitre – jellemzően 1Ft-ra. Így ha el is lopják a kártyaadatainkat valamelyik kereskedő számítógépes rendszeréből, nem férnek hozzá a számlán tartott összegünkhöz. Ott, ahol alszámlához kapcsolódik a kártya, ott annyit költhetünk (és annyit lophatnak el tőlünk), amennyi pénzt előzetesen az alszámlára utaltunk, vagy ott tartunk.



47. ábra VISA Virtual kártya internetes fizetéshez

Egyik legjellemzőbb internetes fizetési módszer még a PayPal, amely egy virtuális számla, amely mögé szintén valamilyen bankkártyát kell megadni. Ha nagyon biztonságos tranzakciót akarunk használni, akkor megadhatunk virtuális kártyát a regisztrációhoz, majd utalhatunk valamennyi összeget a PayPal számlánkra, ennek terhére tudunk majd vásárolni az interneten. Mindeközben a fizikai kártyánk és a bankszámlán tartott pénzünk nincs veszélyben.

Nagyon fontos, hogy akár fizikai (CP – card present), akár internetes fizetésre (CNP – card not present) használjuk a bankkártyánkat, igényeljük a bankunktól a kártyaőr SMS szolgáltatást, amely azért jó, mert azonnal értesülünk arról, ha mi sikeresen vagy sikertelenül fizettünk, illetve ha valamilyen módon kompromittálódott a kártyánk és más szeretne a kártyaadatainkkal visszaélve fizetni. Ebben az esetben azonnal meg tudjuk tenni a szükséges lépéseket. A telefonunkban legyen eltárolva a bankunk kártya ügyfélszolgálatának telefonszáma az azonnali kártyatiltáshoz.

6.7.4 Elektronikus pénz és elektronikus pénztárcák

Az internet világában az elektronikus fizetések lebonyolításához olyan módszereket kellett találni, melyek a készpénzes vagy hagyományos banki átutalásos tranzakciók internetes alternatívájaként – jellemzően a kis összegű (1 eurocent és 25 euro közötti összegekre) – funkcionálhattak. Az elektronikus pénz formáját tekintve digitális adat, ami nem jelentett újdonságot a banki számlavezető rendszerek bevezetését és a hagyományos papír alapú főkönyvek elektronikussá válását követően. Az elektronikus pénznek két fajtája jött létre, az egyik a kártyapénz (pl. HelloPay kártyák) a másik a hálózati pénz (pl. PayPal) [x]. A kártyapénz esetében a pénzt a kártyán lévő mikrochip tárolja – esetenként csak korlátozott ideig, míg a hálózati pénzen egy szerveren működő alkalmazás tartja nyilván az elkölthető egyenleget. Közös a két esetben az, hogy a pénz elköltése kizárólag a feltöltést követően valósulhat meg, ami viszont lehet előzetes (kártyapénz) vagy utólagos (hálózati pénz) egyaránt.

Az elektronikus pénz kibocsátása pénzügyi szolgáltatásnak minősül Európában – de nem számít betétgyűjtésnek, így csak erre feljogosított szervezetek végezhetik. A jogszabály az elektronikus pénz definícióját az alábbiakban határozta meg:

> *„az elektronikus pénz kibocsátójával szembeni követelés által megtestesített, elektronikusan tárolt - ideértve a mágneses tárolást is - összeg, amelyet pénzeszköz átvétele ellenében bocsátanak ki a pénzforgalmi szolgáltatás nyújtásáról szóló törvényben meghatározott fizetési műveletek teljesítése céljából, és amelyet az elektronikus pénz kibocsátóján kívül más természetes és jogi személy, jogi személyiség nélküli gazdasági társaság és egyéni vállalkozó is elfogad, ide nem értve az olyan specifikus készpénz-helyettesítő fizetési eszközökön alapuló szolgáltatásokat, amelyek csak korlátozott módon (zárt körben vagy szűkkörűen) használható eszközön tárolják az adataikat, vagy az elektronikus hírközlő hálózat üzemeltetője vagy az elektronikus hírközlési szolgáltatás nyújtója általi fizetési műveletre használt értéket.”*[16]

Az elektronikus pénz lényeges tulajdonsága tehát, hogy egyrészről fedezetet (feltöltést) igényel, másrészről széles körben elfogadják, mint fizetőeszköz. Például a PayPal felhasználóinak a száma 2010-ben 84,3 millió volt, mely 2018-ra 237 milliós táborra duzzadt [y].

A PayPal olyan hitelintézeti szolgáltatást nyújt, mely lehetővé teszi regisztrációt követően azt, hogy a felhasználók a bejelentkezést követően pénzügyi tranzakciókat hajthassanak végre – jellemzően kisértékű vásárlásokat vagy pénzküldéseket, illetve pénzküldemények fogadását –minden más eszköz használata nélkül. A hálózati elektronikus pénz természetesen bármikor visszaváltható a felhasználó bankszámlájára vagy bankkártyájára. Érdekesség, hogy ha egy tranzakcióhoz nincs elegendő fedezet a felhasználó PayPal számláján, akkor lehetősége van automatikus fedezetfeltöltésre a saját bankszámlájáról [z]. Fontos még tudni, hogy az elektronikus pénz a készpénzzel egyenértékű fizetőeszköz, így az európai törvények értelmében kamatszerzésre nem használható az elektronikus pénzre vonatkozó európai irányelv 12. cikke szerint[17].

A bankkártyás tranzakciók emelt szintű biztonsága érdekében fejlesztették ki a 3D-Secure hitelesítési módszert, mely egy biztonsági protokoll, amely fokozott biztonságot és megbízható hitelesítést nyújt az internetes vásárlásnál a bankkártyák vagy hitelkártyák

---

[16] 2013. évi CCXXXVII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról, 6. § (1) 16.

[17] AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2009/110/EK IRÁNYELVE (2009. szeptember 16.) az elektronikuspénz-kibocsátó intézmények tevékenységének megkezdéséről, folytatásáról és prudenciális felügyeletéről, a 2005/60/EK és a 2006/48/EK irányelv módosításáról, valamint a 2000/46/EK irányelv hatályon kívül helyezéséről (EGT-vonatkozású szöveg)

használatakor. Ezt a különböző kártyatársaságok más-más névvel illették, például „MasterCard SecureCode”, „Verified by Visa”, „J/Secure” a Japan Credit Bureau esetében, illetve American Express kártyák esetén „Safekey”. A 3D-Secure speciális biztonsági kódját a kártyakibocsátó banknak kell meghatároznia és eljuttatnia az ügyfelekhez, hogy a bank engedélyezze az online tranzakciót. A kártyakibocsátó bankok különböző módszerekkel állítják elő és kézbesítik ezeket a kódokat az ügyfelek számára, mellyek igazolni tudják, hogy az internetes regisztrációhoz vagy tranzakcióhoz használni kívánt bankkártyának valóban az adott felhasználó a jogos tulajdonosa. Az EU-ban 2015. augusztus 1. óta minden fizetési szolgáltató számára elvárás a 3D-Secure rendszer támogatása és betartatása.[18]

A mobiltárca egy olyan elektronikus pénztárca, mely a SIM-kártyán elhelyezett speciális chip segítségével tárolja a felhasználó bankkártyájának az adatait és képes azt szolgáltatni elektronikus fizetési tranzakciókhoz mobilalkalmazások vagy NFC leolvasók számára. A chiphez csak az arra felhatalmazott alkalmazások képesek hozzáférni a fizetési tranzakció elindításakor. A biztonság növelése érdekében be lehet állítani egy négyjegyű PIN kódot, amely beírása nélkül nem lehetséges a mobiltárcás fizetés. A biztonságot tovább növelheti a képernyőzár aktiválása is a mobilalkalmazások esetében. Érdekesség, hogy a Vodafone Pay akkor is használható, ha a telefon ki van kapcsolva, vagy lemerült a telefon akkumulátora, mivel fizetéskor a SIM-kártya tartja a kapcsolatot a bankkártya terminállal passzív módon. A magas mobilpenetráció maga után vonta a mobilfizetések előretörését Kínában is, ahol ma már többen fizetnek mobiltelefonnal, mint bankkártyával. A mobilpénztárca használatának van egy adatvédelmi szempontból előnyösnek nevezhető tulajdonsága, nevezetesen a tranzakciónál a vevő adatai helyett a mobiltárca üzemeltetője jelenik meg, így a pénzügyi tranzakciókból nem lehetséges az egyes vásárló szokásait profilírozni, megismerni.

6.7.5 Csaló webáruházak

Ahogy növekszik az internetes vásárlások darabszáma és értéke, úgy jellennek meg azon csaló webáruházak is, amelyek az óvatlan vagy éppen hiszékeny felhasználókat kívánják megkárosítani.

Ha hamis webáruházban vásárolunk, akkor nem csak a kártyával kifizetett összegnek mondhatunk búcsút, hanem az oldalon megadott személyes adatokkal is visszaélhetnek, a

[18] https://en.wikipedia.org/wiki/3-D_Secure

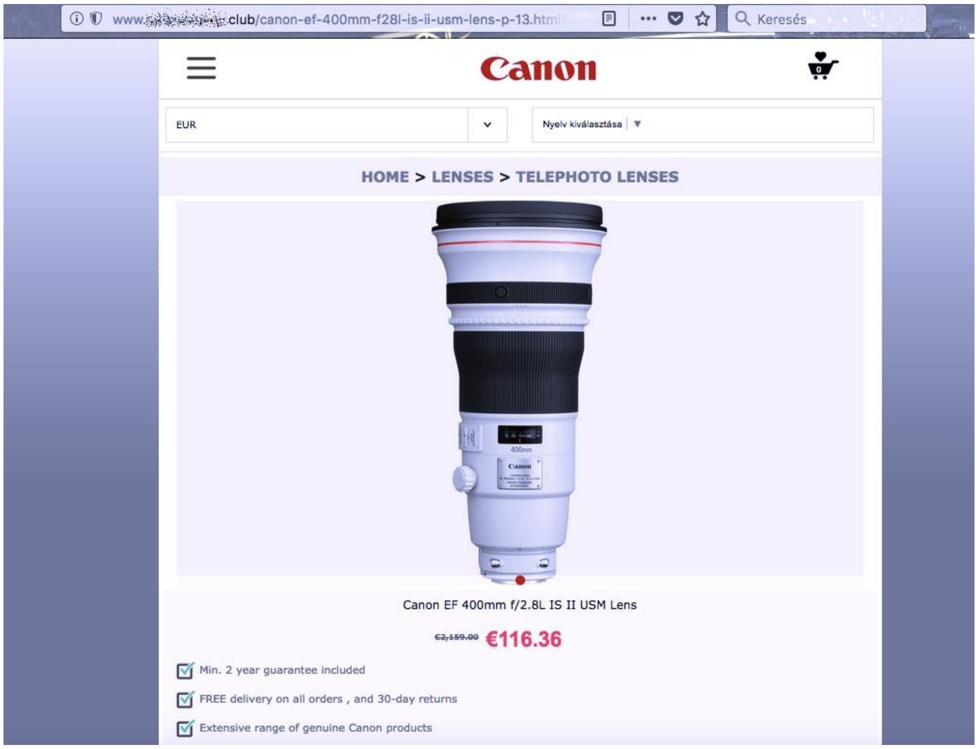
megadott kártyaadatokkal pedig a tulajdonos hozzájárulása nélküli tranzakciókat kezdeményeznek a csalók és/vagy eladják a megszerzett adatokat az interetes feketepiacok valamelyikén. Fontos megkülönböztetni a csaló webáruházakat és a hamis termékeket forgalmazó webáruházakat. Míg utóbbinál van szállítás, csak hamisítványt kapunk, addig az előzőnél a kifizetett áru sohasem érkezik meg és még az adatainkat is ellopják.

Az alábbiakban felsoroljuk, hogy miről ismerhetjük fel a csaló webáruházakat.

- Az első és legfontosabb: az ár túl szép, hogy igaz legyen - Ez a valóságban azt jelenti, hogy milliós fényképezőgépek és objektívek, többszázezer forintos drónok vagy quadok kerülnek egyes oldalakon pár tízezer forintba, míg neves ruha és cipő márkák darabjai párezer forintért megtalálhatóak. Mindezt tetézik a csalók a világon bárhova történő ingyenes házhoz szállítással.
- Nagyon egyszerű weboldal dizájn - A csalók nem fektetnek sok energiát a webáruház kinézetébe, hiszen a bomba ár úgyis elviszi a figyelmet - és sajnos az áldozatok pénzét is.
- Gyanúsan túl nagy választék - Legyen szó ruházati vagy műszaki cikkekről, minden márka minden terméke megtalálható az oldalon. Ez irreális, hiszen az elektronikus kereskedelemnek is megvannak a maga méretgazdaságossági szempontjai.
- A visszafizetési szabályok hiánya, vagy tisztázatlansága - A csaló weboldalak jellemzően másoktól lopják az ilyen szövegeket, vagy annyira általánosak, irreálisak, hogy nem sokra megyünk velük.
- Hamis, vagy nem létező kapcsolati információk - Létező eset, hogy egy hamis webáruház oldalán egy repülőtér teherportájának a címe volt telephelyként megadva, sőt, előfordult, hogy egy létező személy – egy hasonló termékeket forgalmazó másik cég alapítója volt megadva kontaktnak. Érdemes a címnek utánanézni a Google Maps-en, a kontakt névnek és cégnek pedig általában az interneten.
- Csak lelkendező és pozitív kommentek és értékelések - Közösségi oldalakon terjedő hamis áruházaknál érdemes kritikus szemmel nézni a visszajelzéseket. Jellemzően hamis profilokról érkeznek lelkendező kommentek, mindenki elégedett, az összes terméket csodálják és magasztalják – ilyen esetben legyünk résen, mert ez nem életszerű.
- Hamis weboldal cím - A hamis webáruházak vagy egy eredeti termékweboldalhoz hasonló nevet regisztrálnak, kiegészítve valamilyen szóval - például „sales” -, vagy egy-két betű eltéréssel regisztrálják a nevet, amivel könnyen átejthető egy

tájékozatlan vásárló. Például a www.michaelkors.com egy eredeti weboldal, de két „r"-rel www.michaelkorrs.com címről már egy hamis, vélhetően vírusos alkalmazás letöltését ajánló oldalra kerülünk. Erősen javasoljuk, hogy ezen hivatkozást a kedves olvasó NE látogassa meg!

- Semmitmondó webcím, gyanúsan olcsó árukkal, hatalmas kedvezményekkel - Gyanús lehet például az „srostore.com" is, ahol közel 90 százalékos kedvezménnyel kínálnak mindent, motorcsónaktól kezdve a golffelszerelésig. Ha ilyet látunk, érdemes az Amazon-on vagy valamelyik megbízható webáruházban leellenőrizni, hogy ott mennyiért adják a terméket, mert csodák nincsenek.
- Adattisztaság - A hamis weboldalak általában nem foglalkoznak a felhasználói adatok helyességével – hiszen soha nem fognak semmit kiszállítani. Az adatok megfelelőségét egyedül a kártyaadatoknál nézik, amit azonnal le is terhelnek az árucikk árával, azonban szállítás nem történik. Erről tanúskodnak például a scamadviser.com oldalon a hozzászólók panaszai is.



48. ábra Hamis webáruház, gyanúsan olcsó ár. Az objektív valós ára 12.000 EUR körül van

Ha fenti szempontok megvizsgálása után még mindig kétségeink vannak, akkor ellenőrizzük le a megvásárolandó termék árát más webáruházakban. Ha irreális a

különbség, akkor gyanakodjunk! Magát az adott weboldalt is leellenőrizhetjük. Több szolgáltató is foglalkozik azzal, hogy kockázatosnak ítélt weboldalakról szolgáltat információt. Az egyik ilyen a https://transparencyreport.google.com/safe-browsing/search/, de kifejezetten a csaló weboldalakra figyelmeztet a https://www.scamadviser.com/ is.

A másik nagyon egyszerű módszer a weboldal címét és a „scam" (csalás) szavakat gépeljük be a keresőprogramunkba. Ha valóban csaló webáruházzal van dolgunk, akkor jó eséllyel már mások is erre a következtetésre jutottak és jelezték akár kommentekben, közösségi oldalakon, vagy akár a fenti csaló weboldalakat listázó oldalak valamelyikén.

Az internetes vásárlásokhoz használjunk elkülönített számlát, amire csak annyi pénzt teszük, amennyit el akarunk költeni, vagy használjunk internetes kártyát.

Amennyiben megkárosítottak bennünket forduljunk bankunkhoz. Amennyiben azt tapasztaljuk, hogy a kártyaadatainkkal visszaéltek és jogosulatlan tranzakciók történtek, szintén forduljunk bankunkhoz és tiltassuk le az érintett kártyát.

6.7.6 Hamis hírek (fake news) felismerése

A hamis hírek felismerése azért fontos terület, mert nagyjából ugyanazokat a készségeket kell elsajátítani a felismerésükhöz, mintha egy adathalász levelet, vagy csaló webáruházat vizsgálnánk. Bár a hamis hírek közvetlenül nem okozzák az adataink bizalmasságának, sértetlenségének vagy rendelkezésre állásának elvesztését, mégis befolyásolni tudják gondolkodásunkat, ezáltal a világról és egyéb témákról, népcsoportokról, országokról, eseményekről, vagy más, a mindennapi életünkre ható dolgokról alkotott véleményünket. Az alábbiakban pontokba szedjük, hogy milyen szempontok alapján tudjuk eldönteni, hogy hamis vagy valós hírrel állunk szemben:

- Mérlegeljük a forrást, hogy megértsük az oldal küldetését és célját. Rengeteg olyan oldal van, amely más hírportálok nevét kiegészítve próbálja megtéveszteni az olvasókat.
- Nézzük meg a portál többi hírét. Ha jellemzően bulváros, szenzációhajhász, elfogult, áltudományos, konteós/összeesküvés elméletes, túlzottan szatirikus semmitmondó hírek vannak körbevéve reklámokkal, akkor gyanakodjunk, hogy be akarnak csapni.
- Keressük meg az Impresszumot. Az Impresszumban találhatók normális esetben az oldal, hírportál szerzői gárdájának (főszerkesztő, kiadó, rovatvezető stb.) elérhetőségei. Ha nincs impresszum, vagy csak egy e-mail cím van ott, akkor gyanakodjunk.

- Ellenőrizzük a szerző kilétét. Keressünk rá a nevére, hogy megtudjuk, egyáltalán létezik-e, és hihető forrásnak számít-e, vagy éppen álnevet használ. Ha nincs szerző, akkor az is beszédes, hiszen az újságírói etikett megköveteli, hogy névvel publikálják a cikkeket.
- Ha vannak hivatkozások, nézzük meg, hogy azok hova mutatnak. Ha reklámokkal teletűzdelt, hasonló szenzációhajhász oldalra, akkor nagy valószínűség szerint átverés a hír.
- Ellenőrizzük a dátumot. Ez szintén fontos, hiszen előfordul, hogy egy évekkel korábbi hír kezd el önálló életet élni az interneten. Ha nincs dátum és több gyanús körülmény is van, akkor szinte biztos, hogy nem valós hírrel van dolgunk.
- Tompítsuk saját előítéletünket annak érdekében, hogy megnézzük, a hír befolyással van-e az ítélőképességünkre. Irányul-e bármilyen csoport, népcsoport, ország, eszme, esemény stb. ellen?
- Keressünk rá a hírre más neves hírportálokon. Ha nyoma sincs például egy olyan eseménynek, ami egyébként országos érdeklődésre tartana számot, akkor valószínű, hogy álhírrel van dolgunk.
- Ha a hírhez kép is van mellékelve, mentsük el és töltsük fel a képet a Google képkeresési funkciójába és keressünk rá, hogy máshol, más oldalakon megtalálható-e? Ilyen esetekben gyakran előfordul, hogy a kép egész más esemény, ország vagy hír kapcsán lett publikálva, ráadásul, ha dátumilag is eltérés van, akkor szinte biztos, hogy a kép lopott és valószínű, hogy a hír is hamis.
- Ha olyan hírrel találkozunk a közösségi oldalon, amely a tényleges elolvasás előtt már megosztást kér, akkor gyanakodjunk, hogy álhírrel van dolgunk és az egész csak az adott oldal (és a rajta lévő reklámok) népszerűségét szolgálja.
- Az ilyen hírek címének jellemzői az alábbi szófordulatok: „Nem fogod elhinni…”, „A híres sztárral olyan dolog történt, hogy eláll a szavad…”, A neves riporter valamit talált, de ami ez után történt, arra nincsenek szavak…” Tehát semmi konkrét nem derül ki a címből, de az olvasó érzelmeire, kíváncsiságára próbál hatni a hír.

Egy klasszikus ilyen főcím, kérjük a kedves olvasót, hogy a fentiek alapján ítélje meg, hogy ez egy igazi vagy hamis hír lehet? „Egy hatalmas elhagyatott hajóroncsot találtak a Aggteleki Nemzeti Parkban! Mikor átkutatták a fedélzetet feldolgozhatatlan látvány tárult a szemük elé!”

6.7.7 Internetes zaklatás

Az internetes zaklatás – gyermekeket és felnőtteket is ideértve – az internetes világunknak egyik legnagyobb és egyre gyakoribb problémája. Az internetes zaklatás – bántalmazás a virtuális térben, az infokommunikációs technológia felhasználásával (internetes oldalak, közösségi portálok, fórumok, e-mail, SMS, azonnali üzenetküldők).

6.7.7.1 A zaklatásnak számos típusa ismert és kategorizált:

- Zaklatás: támadó, sértő, felzaklató üzenetek küldése sorozatosan
- Lejáratás – rossz hírnév terjesztése: Valótlan pletykák terjesztése, amelyek megszégyenítik, lejáratják a másikat. (akár pl. hamis fényképek terjesztése)
- Flaming: online „háború", támadás, veszekedés: dühös, támadó, trágár hozzászólások nyilvános fórumokon (gyakran online politikai, vallási, ideológiai vita)
- Identitáslopás: Az áldozat e-mail címének, vagy közösségi oldalon a profiljának feltörése azzal a szándékkal, hogy a nevében küldjön sértő, kellemetlen üzenetet másoknak
- Kiközösítés: Az online közösség egy tagjának a csoportból való kirekesztése
- Kibeszélés: titkok megosztása, személyes információk nyilvánosságra hozása, elküldése
- Becsapás: A másik becsapása, kellemetlen vagy intim információk kicsalása majd megosztása.
- Cyber Stalking: fenyegető, megfélemlítő üzenetek küldése, a másik online szokásainak megfigyelése és ezek felhasználása félelemkeltésre, hogy a másik a saját biztonságát veszélyeztetve érezze
- Sexting: szexuálisan provokatív fényképek, videók készítése, és továbbküldése

6.7.7.2 Internetes zaklatás lehetséges okai:

- Anonimitás/személytelenség. A támadó azt gondolja, hogy láthatatlan tud lenni, kicsi a lebukás veszélye
- Kevesebb visszajelzés – eldurvulás. Míg fizikai kontaktusos nézeteltéréseknél a támadó, agresszor látja a másik reakcióit és ez hatással is tud lenni rá, addig az online térben elkövetett zaklatásoknál nincs ilyen azonnali visszajelzés, emiatt a támadó sokkal inkább el tudja ragadtatni magát.

- Nincs közösségi visszajelzés. Szintén visszautalva a fizikai veszekedésekre, ha az egy valós közösségben történik, akkor a közösség más tagjai is tudnak visszajelzést adni, amivel meg lehet fékezni adott esetben egy eldurvuló zaklatást. Ilyen a legjobb esetben is közösségi oldalakon vagy csoportokban fordul elő, de sajnos elég sok a szemlélődő, passzív résztvevő, akik inkább nem folynak bele a konfliktusba. A valós fizikai konfliktus esetén ezt nehezebben tudják megtenni és inkább beavatkoznak. Az online térben ezt sajnos el tudják kerülni.
- Személyes kommunikációban lévő fékek hiánya. Személyes kommunikációban azonnal lehet verbális és nonverbális visszajelzést adni, illetve rábírni a támadó felet, hogy hagyja abba, amit csinál.
- Az áldozat nem tud menekülni, hiába van otthon például. Az online világból nem lehet elmenekülni – vagy nagyon nehéz. Nem áll meg az online zaklatás az iskolakapuban vagy a munkahely kijáratánál. Emiatt az áldozat fokozottan rosszul érzi magát, ha pedig mégis kilép az adott virtuális közösségi térből, akkor egyrészt minden információforrást elveszít, másrészt kirekesztettnek érezni magát, ami szintén nagyon rossz.
- Gyorsan nagy nyilvánosság. Egy közösségi megosztással pillanatok alatt kaphat egy zaklatás nagy nyilvánosságot, ami ebben a mivoltában kikerül az eredeti résztvevők kontrollja alól és akár beláthatatlan következményei is lehetnek.
- Nehéz fellépni ellene (felhasználó törlés és tiltás, poszt, fotó törlés, bizonyítás)

6.7.7.3 Interntes zaklatás lehetséges következményei:

Az internetes zaklatás negatív hatással lehet a testi és lelki egészségre, fejlődésre, társas kapcsolatokra, iskolai és sport vagy egyéb teljesítményre egyaránt.

- Düh
- Szorongás
- Depresszió
- Önsértés
- Magányosság
- Iskolakerülés, szökés
- Pszichoszomatikus betegségek
- Alacsony önértékelés
- Öngyilkossági gondolatok/befejezett öngyilkosság (Sajnos számos példa van arra, hogy internetes zaklatás öngyilkosságba torkollott.)

6.7.7.4 Internetes zaklatás kezelési módszerei:

- A zaklató felszólítása, hogy hagyja abba! (legfontosabb – visszajelzés adás)
- Azonnali, praktikus segítségnyújtás (tiltás, törlés, bejelentés)
- Segítségkérés: Kék vonal 116-111, http://www.kek-vonal.hu
- http://www.saferinternet.hu [t] – számos kiváló anyag van gyermekeknek, szülőknek, pedagógusoknak a téma feldolgozására.
- Ha kell, akár pszichológushoz, vagy hatósághoz fordulni

Probléma a kezelési módokkal, hogy a gyerekek jelentős része úgy gondolja, hogy jobban ért az internethez és a technológiához, mint a szülője – pedagógusa. Emiatt sajnos nem fogadnak meg jótanácsokat és nem fogadják el a tiltást, korlátozást büntetést sem.

6.7.7.5 Internetes zaklatás megelőzése

A legfontosabb dolog az internetes zaklatás megelőzése, hogy ismerőseink, családtagjaink, barátaink, de legfőképp gyermekeink ne váljanak se áldozattá, se zaklatóvá. Ennek számos viszonylag egyszerű, ámde időt és energiát igénylő módszere van:

- Felkészülni, megismerni a trendeket, szokásokat, képben lenni! Ha nem vagyunk felkészültek, akkor a gyerek/családtag nem fogad el, nem tőlünk kér tanácsot, segítséget!
- Beszélgetni a gyerekkel, SOKAT beszélgetni – bizalom kiépítése nagyon fontos!
- Felkészíteni a leggyakrabban használt app-ok, szolgáltatások és oldalak BIZTONSÁGOS használatára.
- Ellenőrzés: Elkérni a telefont, gyerekkel együtt átnézni, internet böngésző előzmények, Youtube előzmények, VIBER/Whatsapp/Snapchat/Tinder Messenger csoportokat,
- Facebookon és más közösségi oldalakon (Twitter, Instagram) legyen ismerős a gyerek, hogy tudjuk követni a közösségi aktivitásait
- Szülői felügyelet program használata
- Szabályok lefektetése (pl. telefon használat korlátozása, idegenekkel nem ismerkedünk, nem találkozunk, ésszel publikálunk stb.)

7 Mellékletek

7.1 Ajánlott irodalom

Az ajánlott irodalom időbelisége feltűnhet a kedves olvasónak. Fontos megjegyezni, hogy a lenti irodalomlista a mai napig használatos és alapvető szakmai tartalmakat hordoz. Ugyanakkor számos publikáció, riport, tanulmány, értekezés már nem jelenik meg nyomtatott könyv formájában, ezeket az Interneten keresztül érhetjük el.

[1] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

[2] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; August 2005 Version 2.3 CCMB-2005-08-001

[3] Budapesti Műszaki és Gazdaságtudományi Egyetem Gazdaság- és Társadalomtudományi Kar Információ- és Tudásmenedzsment Tanszék Biztonság Menedzsment Csoport; Az informatikai biztonság fogalmainak gyűjteménye; Ajánlás ; 1.0 változat; 2003

[4] COBIT 4.1 – Control Objectives for Information and Related Technology, 1996-2007 IT Governance Institute

[5] COBIT 5 A Business Framework for the Governance and Management of Enterprise IT, ISACA, 2012

[6] Kevin Mitnick: A behatolás művészete, PERFACT-PRO Kft.; 2006; ISBN: 9789638647252

[7] Andrew S. Tannenbaum: Számítógéphálózatok; Panem–Prentice-Hall, 1999

[8] Ryan Russell: A Háló kalózai – Hogyan lopjunk kontinenst, Kiskapu Kft., 2005; ISBN: 9789639301993

[9] Kevin Mitnick: A megtévesztés művészete, PERFACT-PRO KFT.; 2003;
ISBN: 9789632065557

[10] Kevin Mitnick: A legkeresettebb hacker, HVG Kiadói Zrt., 2012; ISBN: 9789633040898

[11] Simon Singh: Kódkönyv - A rejtjelezés és rejtjelfejtés története, Park Kiadó, 2007; ISBN: 9789635307982

[12] The National Strategy to Secure Cyberspace, February 2003, White House, USA

7.2 Internetes hivatkozások jegyzéke

[a] http://real.mtak.hu/11147/

[b] http://www.govcert.hu/

[c] http://neih.gov.hu

[d] http://hu.wikipedia.org/wiki/Számítógép-architektúra

[e] http://en.wikipedia.org/wiki/Cloud_computing

[f] legnépszerűbb weboldalak http://24.hu/media/2016/08/01/ezek-a-legnepszerubb-weboldalak-a-magyar-es-a-tersegbeli-fiatalok-koreben

[g] http://www.magyarorszag.hu

[h] jelszótörés - 10 millió jelszó https://xato.net/today-i-am-releasing-ten-million-passwords-b6278bbe7495

[i] Symantec 2017 Threat Report https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

[j] makró http://wiki.prog.hu/wiki/Makr%C3%B3

[k] Adatvédelmi irányelv http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:hu:HTML

[l] DNS https://hu.wikipedia.org/wiki/Domain_Name_System

[m] captcha http://hu.wikipedia.org/wiki/Captcha

[n] Biztonságos törlés http://www.howtogeek.com/72130/learn-how-to-securely-delete-files-in-windows/

[o] PGP http://hu.wikipedia.org/wiki/PGP

[p] Global Use of Electronic Authenticity; Erdősi Péter Máté, SSRN, 2013; http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2264335

[q] Szünetmentes táp https://www.pcx.hu/szunetmentes_tap

[r] Windows Backup http://www.backup-utility.com

[s] TimeVault http://www.tucows.com/preview/722287/Time-Vault

[t] http://www.saferinternet.hu

[u] https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-wi-fi-certified-wpa3-security

[v] https://index.hu/tech/2018/07/11/a_leheto_legnagyobb_birsagot_kapta_a_facebook_a_cambridge_analytica...

[w] http://www.origo.hu/gazdasag/20180712-a-facebook-az-oroszoknak-is-adott-el-felhasznaloi-adatokat...

[x] http://www.bankszovetseg.hu/Content/Hitelintezeti/034Szeplaki.pdf

[y] https://www.statista.com/statistics/218493/paypals-total-active-registered-accounts-from-2010/

[z] https://www.paypal.com/hu/webapps/mpp/ua/servicedescription-full?locale.x=hu_HU